Universidad de Valladolid

Facultad de **Derecho**

Grado en **Derecho**

La difícil articulación de garantías de protección de los datos personales transferidos desde la Unión Europea a terceros países. Análisis y consecuencias de las Sentencias Schrems I y Schrems II del Tribunal de Justicia de la Unión Europea

Presentado por:

Nicolás Cabezudo Vidal

Tutelado por:

Juan Fernando Duran Alba

Valladolid, 14 de julio de 2021

ÍNDICE

Resumen

La articulación de mecanismos jurídicos dirigidos a garantizar el derecho fundamental a la protección de datos personales en las transferencias internacionales de datos ha sido uno de los objetivos de la Unión Europea, creando un entramado de instrumentos jurídicos de entre los que destacan las Decisiones de adecuación de la Comisión Europea como mecanismo ideal para garantizar la seguridad de dichas transferencias. Sin embargo, la jurisprudencia del Tribunal de Justicia de la Unión Europea, en sus Sentencias Schrems I y Schrems II, anula sendas Decisiones de adecuación con respecto a Estados Unidos, poniendo de manifiesto que las garantías comunitarias son deficientes y creando incertidumbre en las relaciones comerciales con ese Estado. Actualmente, ante la falta de una Decisión de adecuación que ampare las transferencias internacionales de datos personales dirigidas a Estados Unidos, las empresas deben utilizar los mecanismos alternativos recogidos en el Reglamento General de Protección de Datos, siendo el consentimiento del interesado la cláusula de cierre del sistema.

Palabras clave

Protección de datos personales - Transferencias internacionales de datos personales - Schrems I - Schrems II - Snowden- Puerto Seguro - Escudo de Privacidad - Unión Europea - Tribunal de Justicia de la Unión Europea - Directiva 95/46/CE - Reglamento General de Protección de Datos – NSA - Estados Unidos.

Abstract

The articulation of legal mechanisms aimed at guaranteeing the fundamental right to the protection of personal data in international data transfers has been one of the objectives of the European Union, creating a network of legal instruments, including the European Commission's adequacy decisions as the ideal mechanism for ensuring the security of such transfers. However, the case-law of the Court of Justice of the European Union, in its judgments in Schrems I and Schrems II, annuls each adequacy decision in respect of the United States, demonstrating that Community guarantees are inadequate and creating uncertainty in trade relations with that State. Currently, in the absence of an Adequacy Decision covering international transfers of personal data to the United States, companies should use the alternative mechanisms contained in the General Data Protection Regulation, where the data subject's consent is the system closure clause.

Key Words

Personal data protection - International data transfers - Schrems I - Schrems II - Snowden - Safe Harbour - Privacy Shield - European Union - Court of Justice of the European Union - Directive 95/46/EC - General Data Protection Regulation - NSA - United States

1. INTRODUCCIÓN

Cuando en junio de 2013 Edward Snowden, un joven informático norteamericano que trabajaba para la Agencia de Seguridad Nacional de los Estados Unidos (NSA), descubrió y filtró a la prensa una serie de documentos que probaban fehacientemente la interceptación, por parte del ejecutivo de los Estados Unidos, de conversaciones telefónicas, correos electrónicos y datos de carácter personal de ciudadanos norteamericanos y de terceros países (todo ello sin conocimiento de los interesados, sin cobertura legal y sin autorización judicial, simplemente amparado en genéricos "intereses relacionados con la seguridad nacional"), resultó evidente la ilegítima intervención de la potencia americana en la privacidad de la población mundial[1].

A través de las revelaciones de Snowen se conoció la existencia en Estados Unidos de varios programas de vigilancia estatal (como los programas PRISM[2] y Upstream[3]), mediante los que la NSA interceptaba masivamente datos personales de ciudadanos de la Unión Europea transferidos desde empresas privadas europeas a empresas privadas norteamericanas, lo que se conseguía interviniendo los cables de fibra que conectan el Continente Europeo con los Estados Unidos y accediendo impunemente a bases de datos personales de las empresas y entidades norteamericanas.

Como se recordará, las filtraciones de Snowen provocaron una ola de indignación y duras críticas contra las autoridades norteamericanas por parte de gobiernos de terceros

---

[1] La primera noticia sobre esta cuestión se publicó en el periódico *The Guardian* el 13 de junio de 2013 [https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance]. Véase LEFÉBURE, A.: *El Caso Snowden: así espía Estados Unidos al mundo*. Clave intelectual, Madrid, 2014.

[2] Con el término PRISM se calificaba un programa secreto de vigilancia electrónica utilizado por la Agencia de Seguridad Nacional de los Estados Unidos, que tenía como objetivo la recogida masiva de datos de ciudadanos de todo el mundo contenidos en los ficheros electrónicos de compañías de telecomunicaciones estadounidenses. Los documentos sustraídos por Snowen probaron que la NSA accedía a la información almacenada en los servidores de al menos nueve firmas con gran peso en Internet, como son *Microsoft, Yahoo!, Google, Facebook, PalTalk, YouTube, Skype, AOL y Apple. Véase:* Glenn Greenwald; Ewen MacAskill: «NSA Prism program taps in to user data of Apple, Google and others». The Guardian, 7 de junio de 2013 [https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data].

[3] Según la información filtrada por Snowden, la NSA utilizaba el término *Upstream* para referirse a sus sofisticados programas de vigilancia que recogen información obtenida a través de las comunicaciones realizadas mediante cables de fibra. Concretamente los programas FAIRVIEW, STORMBREW y BLARNEY recopilan datos personales de ciudadanos norteamericanos o residentes en este país, mientras que el programa OAKSTAR recoge datos personales de ciudadanos de terceros países.

países, de ciudadanos y de empresas y, en lo que ahora nos interesa, en el ámbito de la Unión Europea la Comisión Europea se vio en la necesidad de redactar, el 27 de noviembre de 2013, una Comunicación al Parlamento Europeo titulada "Restablecer la confianza en los flujos de datos entre la UE y EE.UU", en la que se ponía de manifiesto que los Estados Unidos ya no resultaban un *Puerto Seguro* para los datos personales de los ciudadanos comunitarios (aludiendo así al *Acuerdo de Puerto Seguro* suscrito en el año 2000 entre la Unión Europea y Estados Unidos, amparado en la Decisión de Adecuación de la Comisión 200/520/CE, de 26 de julio de 2000*,* mediante la que la Unión Europea certificaba que las empresas norteamericanas que suscribían este acuerdo garantizaba un nivel de protección de los datos de carácter personal similar al existente en la Unión Europea).

No obstante, la Comisión no anuló la citada Decisión de adecuación, pues las consecuencias para las relaciones comerciales entre los Estados Unidos y la Unión Europea podrían ser nefastas. El flujo de transferencias de datos entre ambos países continuó hasta que un ciudadano austriaco, el Sr. Schrems, usuario de la red social *Facebook* (empresa con domicilio social en Estados Unidos), se negó a aceptar que las autoridades norteamericanas pudieran acceder, de manera indiscriminada, a los datos personales que los usuarios de la red social volcaban con acceso restringido, por lo que, emulando el mito de David contra Goliat, inició una batalla legal contra *Facebook Inc.*, acusando a la empresa de no proteger debidamente sus datos personales, lo que finalizó con sendas Sentencias del Tribunal de Justicia de la Unión Europea (SSTJUE): la STJUE Schrems I, de 15 de julio de 2015 (Gran Sala)[4], y la STJUE 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 Europeo relativa a la protección de datos de carácter personal, cuyo análisis y consecuencias constituyen el objeto principal de este trabajo, puesto que nos ofrecen una interesante información acerca de la dificultad de fijar medidas jurídicas de protección que resulten eficaces cuando los datos personales traspasan las fronteras de la Unión.

La articulación de garantías de protección de los datos personales transferidos desde la Unión Europea a terceros países cuenta con dificultades de diversa naturaleza, de entre las que hay que destacar la complejidad técnica, cada vez más sofisticada, de lo que se ha venido a calificar como "tecnologías disruptivas"[6], a lo que se une el fenómeno de la globalización.

[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).

[6] Se utiliza el adjetivo *disruptivas* para calificar a las "nuevas tecnologías" que se caracterizan por una radical innovación, que deja obsoleta la tecnología anterior, de ahí el término *disruptivo*, pues se produce una ruptura

Así, por un lado, los avances tecnológicos permiten que empresas privadas y autoridades públicas puedan realizar 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[7], 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[8], pues el mundo digital carece de fronteras geográficas, los distintos Estados cuentan con muy diversos estándares de protección de los datos de carácter personal y los prestadores de bienes o servicios *online*, que pueden fijar su sede en cualquier lugar geográfico, ostentan una posición dominante en el mercado, frente a unos ciudadanos en una clara situación de inferioridad.

Por todo ello, tal y como se intentará argumentar a lo largo de este trabajo, la protección de los datos de carácter personal necesita de una regulación supranacional y, en este sentido, la Unión Europea (UE) 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 sólo dentro de la Unión, sino también cuando estos 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 de los datos garantice un nivel de protección sustancialmente equivalente al existente en la Unión Europea, pues cuando los datos personales circulan a través de las fronteras hacia el exterior de la Unión, disminuye la capacidad de los ciudadanos

brusca, un cambio profundo en las formas de comunicación, de comercio, de sistemas de trabajo, etc. Las tecnologías disruptivas tienen como denominador común la capacidad de evolucionar rápidamente y de adaptarse a diferentes sectores, generando nuevos modelos de comercio (son ejemplos claros el *Big data*, la inteligencia artificial, la prestación de servicios de *cloud computing*, la tecnología *blockchain*, etc.).

[7] *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*), entre otros.

[8] Utilizamos en término "tratamiento" de datos de carácter personal en el sentido en el que lo hace el vigente Reglamento Europeo en su art. 4.2: "cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción".

comunitarios para ejercer el derecho fundamental a la protección de datos garantizado en la Carta de Derechos de la Unión Europea y en las distintas constituciones de los Estados miembros. Sin embargo, como se razonará a lo largo de las siguientes líneas, la eficacia real de dichos mecanismos de protección deja mucho que desear.

2. LA PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL COMO DERECHO FUNDAMENTAL EN EL ÁMBITO DE LA UNIÓN EUROPEA

El Tratado de Lisboa, firmado el 13 de diciembre de 2007 por los Estados miembros de la Unión Europea[9], constituye un paso definitivo en el "prolongado esfuerzo por revestir la construcción europea de dimensión constitucional"[10], no sólo 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, tal como fue adaptada el 12 de diciembre de 2007 en Estrasburgo, la cual tendrá el mismo valor jurídico que los Tratados" (art. 6 TUE).

Asimismo, con la entrada en vigor del Tratado de Lisboa, la Unión reconoce el valor del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (art. 6.2 TUE) y establece que: "Los derechos fundamentales que garantiza el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales y los que son fruto de las tradiciones constitucionales comunes a los Estados miembros formarán parte del Derecho de la Unión como principios generales" (art. 6.3 TUE)[11]. Hay que tener en cuenta, como ha tenido ocasión de declarar el Tribunal de Justicia

[9] 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.

[10] LÓPEZ AGUILAR, J. F.: "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-EUUU". *Teoría y Realidad Constitucional*, núm. 39, UNED, 2017, p. 557.

[11] Para una mayor profundización sobre esta cuestión puede consultarse, entre otros muchos: BALAGUER CALLEJÓN, F.: "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, Dykinson, Madrid, 2008, pp. 133-157; y CARMONA CONTRERAS, A.: "El espacio europeo de los derechos

de la Unión Europea (en adelante TJUE), que, aunque los derechos contenidos en la Carta que se correspondan con derechos garantizados por el Convenio Europeo de Derechos Humanos (en adelante CEDH) tienen el mismo sentido y alcance que les confiere dicho Convenio, este no constituye un instrumento jurídico integrado formalmente en el ordenamiento jurídico de la Unión, dado que la Unión no se ha adherido formalmente a él[12].

A los efectos de este trabajo, nos interesa reparar en la importancia de la incorporación de la Carta de los Derechos Fundamentales de la Unión Europea (CDFUE)[13] (como derecho vinculante para las instituciones, órganos y organismos de la Unión, así como para los Estados miembros cuando apliquen el Derecho de la Unión[14]), 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, LÓPEZ AGUILAR afirma que: "Los estudios más recientes de la doctrina especializada señalan al menos tres ámbitos específicos de incidencia decisiva de la jurisprudencia del TJ sobre la de los tribunales garantes de los ordenamientos de los EEMM: el acceso a la Justicia y a la tutela judicial; la igualdad de trato y no discriminación; y, en lo que nos ocupa, privacidad, vida privada y protección de datos"[15].

Pues bien, centrándonos en el último de los ámbitos señalados (privacidad, vida privada y protección de datos), es de señalar que el artículo 7 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 CDFUE reconoce a toda persona "el derecho a la

fundamentales: de la Carta a las constituciones nacionales", *Revista Española de Derecho Constitucional*, núm. 7, CEPC, Madrid, 2016, pp. 13-40.

[12] SSTJUE de 26 de febrero de 2013, Akerberg Fransson (C-617/10, EU: C:2013:105), apartado 44 y jurisprudencia citada, y de 20 de marzo de 2018, Menci (C-524/15, EU:C:2018:197), apartado 22.

[13] 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.

[14] Tras su entrada en vigor se suscitaron algunas dudas respecto del carácter vinculante de la Carta, como indica ROLDAN BARBERO, J.: "La Carta de los Derechos Fundamentales de la Unión Europea: su estatuto constitucional", *Revista de Derecho Comunitario Europeo*, núm. 16, septiembre-diciembre, 2003, p. 947. Sin embargo, con los años los efectos jurídicos vinculantes de la Carta no se cuestionan pues, como señala Araceli Mangas, "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", en: MANGAS MARTÍN, A.: "Comentario al artículo 51", en *Carta de los Derechos Fundamentales de la Unión Europea: comentario artículo por artículo* (Dir.: Mangas Martín), Fundación BBVA, 2008, p. 814.

[15] *Op. cit.*, p. 559. Sobre el importante papel del TJUE en la defensa de los Derechos de la Carta puede consultarse: SÁIZ ARNÁIZ, A.: "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 *Constitución europea y constituciones nacionales* [Gómez Fernández, I. (coord.)/Cartabia, M. (dir.)/De Witte, B. (dir.)/Pérez Tremps, P. (dir.)], Tirant lo Blanch, Valencia, 2005, pp. 531-588.

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 art. 8 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 intentará exponer a lo largo de este trabajo (mediante el análisis de algunas Sentencias 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 datos personales, que no son sólo aquellos que pueden calificarse como íntimos, sino toda información relativa a una persona física identificada o identificable[16].

También debemos destacar que en los primeros años de vigencia de la Carta algunos autores consideraron que no quedaban suficientemente garantizados algunos principios vinculados a la protección de datos personales, como los de "información, control, seguridad y confidencialidad"[17], pero lo cierto es que, como intentaremos argumentar, la regulación de la Unión Europea que desarrolla este derecho es exhaustiva y rigurosa, otra cosa distinta, como también se intentará explicar, es que resulte eficaz cuando se trata de proteger los datos personales de los ciudadanos comunitarios una vez que sobrepasan las fronteras de la Unión y llegan a un tercer Estado.

Asimismo, debemos señalar que, conforme al art. 52.1 CDFUE, cualquier limitación del ejercicio de los derechos y libertades reconocidos por la Carta deberá estar prevista en la ley y respetar el contenido esencial de dichos derechos y libertades, lo que ha de completarse con lo previsto en el art. 52.1 CDFUE, en el que se indica que, atendiendo al principio de proporcionalidad, sólo podrán introducirse limitaciones a dichos derechos y libertades cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos

[16] Como recogía, con anterioridad a la entrada en vigor de la carta, la Directiva 95/46/CE, en su art. 2 a).

[17] Véase, RUIZ MIGUEL, C.: "El derecho a la protección de datos de carácter personal en la Carta de Derechos Fundamentales de la Unión Europea: Análisis crítico", *Revista de Derecho Comunitario Europeo,* núm. 14, enero-abril, 2003, p. 39.

por la Unión o a la necesidad de protección de otros derechos y libertades reconocidos en la carta.

Pues bien, aplicando esos principios a la protección de datos de carácter personal y con la finalidad de exponer, en esta primera parte del trabajo, algunas líneas generales de la jurisprudencia del TJUE en relación con esta materia, es de señalar que el Tribunal de Justicia ha venido sosteniendo que, para cumplir el requisito 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"[18]. 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[19].

El Tribunal de Justicia también ha declarado en numerosas ocasiones que la comunicación de datos de carácter personal a un tercero (tanto si es una autoridad pública, como si se trata de un particular), sin consentimiento del interesado y con una finalidad distinta a aquella para la que fueron recogidos, constituye una injerencia grave en los derechos fundamentales consagrados en los artículos 7 y 8 de la Carta, con independencia de que tales datos sean o no de carácter personal[20]. Por ello, es lugar común entre la doctrina subrayar que la jurisprudencia del TJUE dictada en materia de protección de datos ha tenido una influencia decisiva para la configuración del contenido de este derecho y para los Tribunales Constitucionales de los Estados miembros: "el TJUE ha venido estableciendo en estos últimos años una jurisprudencia, en su conjunto, sólida e incisiva, interpretando los derechos de los arts. 7 y 8 CDFUE, con una aproximación asertiva y decididamente favorable a la garantía de la privacidad y a los principios europeos de reserva de Ley, de necesidad y de proporcionalidad y legitimidad de la finalidad (*purpose limitation*) junto a la delimitación temporal de la retención y conservación de datos (*retention period*), influyendo tanto en los

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

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

[20] Véanse, en este sentido, la STJUE de 8 de abril de 2014, Digital Rights Ireland y otros (C-293/12 y C-594/12, EU:C:2014:238), apartados 33 a 36.

asuntos (*Case Law*) concernientes a la trasposición de la Directiva de Protección de Datos 95/46 en el Derecho interno, como en los relativos a la aplicación del Derecho de los EEMM"[21].

Lo que nos interesa resaltar desde estas líneas, es 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 sólo dentro de las fronteras de la Unión, sino también respecto de los países terceros a los que se transfieren datos personales, tal y como se desprende de las STJUE Schrems I y II, que comentaremos más adelante.

También creo que 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[22]. Por esa razón, no forma parte de nuestro objeto de estudio el análisis del derecho fundamental a la protección de datos en las Constituciones de los Estados miembros, ni la jurisprudencia dictada por los tribunales constitucionales de dichos Estados que, como ha ocurrido en el caso de España, han tenido un papel muy importante en la configuración del derecho fundamental a la protección de 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, en las que reconoce un derecho fundamental autónomo a la protección de datos de carácter personal, a partir de la redacción del art. 18.4 CE 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". 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 art. 18.4 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)[23].

[21] LÓPEZ AGUILAR, J. F., "La protección de datos personales...", *op. cit.*, p. 561.

[22] Como se indica en la STJUE de 18 de octubre de 2016, Nikiforidis (C-135/15, EU:C:2016:774), apartado 28.

[23] Sobre esta materia puede consultarse, entre otros: AGUADO RENEDO, C.: "La protección de los datos personales ante el Tribunal Constitucional español", *Revista Mexicana de Derecho Constitucional*, núm. 23, julio-diciembre 2010, pp. 3-25. Más recientemente BILBAO UBILLOS, J. M.: "De la relación de las jurisprudencias constitucionales europea y española sobre derechos fundamentales en sus Derechos sustantivos". En XXV

3. LA NORMATIVA EUROPEA DIRIGIDA A LA PROTECCIÓN DE LOS DATOS PERSONALES EN LAS TRANSFERENCIAS INTERNACIONALES DE DATOS

3.1. Algunas cuestiones generales

Como se intentará fundamentar a lo largo de las siguientes líneas, se puede afirmar que, tanto desde el Consejo de Europa, como desde la Unión Europea, se ha asumido la responsabilidad de impulsar instrumentos jurídicos destinado a adaptar el ordenamiento jurídico a la era digital, con la finalidad de articular garantías jurídicas efectivas para la protección de todos los derechos fundamentales, particularmente de aquellos que pueden verse afectados de manera más directa por las tecnologías disruptivas, como el derecho a la intimidad y el derecho a la protección de datos de carácter personal.

No se pretende en este trabajo llevar a cabo un análisis pormenorizado de la normativa europea en materia de protección de datos, pues sólo examinaremos 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 de datos se produce como consecuencia de las relaciones comerciales entre dos o más operadores jurídicos.

En este sentido, es interesante destacar que el Consejo de Europa y la Unión Europea no se han limitado a garantizar, dentro de sus respectivos espacios de competencia, un nivel uniforme de protección de los datos de carácter personal dentro del territorio europeo, sino que también han salido al paso de los problemas derivados de la globalización y de la expansión del comercio internacional, asumiendo que cuando los datos personales atraviesan las fronteras y salen del espacio europeo existe un mayor peligro de que sean vulnerados, por lo que será necesario fijar garantías específicas de protección dirigidas a comprobar que los países terceros cuentan con un nivel de protección adecuado.

Jornadas de la Asociación de Letrados del TC, Cuatro Décadas de Jurisprudencia Constitucional: los Retos. Centro de Estudios Políticos y Constitucionales, Madrid, 2020, pp. 66 y ss.

Como se verá, el celo de los diversos organismos internacionales por garantizar el derecho a la protección de los datos de carácter personal puede llevar al extremo de prohibir o suspender aquellas relaciones comerciales que impliquen un flujo de datos personales hacia terceros países en los que no se cuenta con un estándar de protección adecuado, con el consiguiente efecto negativo en las relaciones comerciales. Sin embargo, como se intentará exponer a lo largo de este trabajo, en la Unión Europea encontramos diversos niveles de protección de datos, hasta llegar a un último escalón en el que la responsabilidad última recae exclusivamente en el interesado, que deberá optar por: (i) continuar con una determinada relación comercial (y autorizar expresamente la eventual cesión y tratamiento de datos a terceros, asumiendo la falta de garantías al respecto, eximiendo así de responsabilidad a las empresas implicadas), o (ii) prescindir de dicha relación comercial, con la finalidad de proteger sus datos de carácter personal.

3.2. Mecanismos de protección del Consejo de Europa

Siguiendo un orden cronológico, la primera referencia normativa relativa a las transferencias internacionales de datos la encontramos en el Convenio núm. 108 del Consejo de Europa, de 28 de enero de 1981, que se aprobó, precisamente, con la finalidad de garantizar a toda persona física (con independencia de su nacionalidad, pero con residencia en un Estado del Consejo de Europa[24]), la protección frente al tratamiento automatizado de los datos de carácter personal.

Este Convenio, firmado hace más de cuarenta años, se considera el primer instrumento internacional, jurídicamente vinculante, adoptado con la finalidad de proteger el tratamiento automatizado de los datos de carácter personal, siendo importante señalar que, ya en este primer momento, los flujos transfronterizos de datos de carácter personal cuentan

[24] El Consejo de Europa nace tras la Segunda Guerra Mundial, con la firma del Tratado de Londres, el 5 de mayo de 1949, con el objetivo de erigirse como guardián de los valores democráticos en el continente europeo, labor que continúa desarrollando en la actualidad. Diez Estados participaron en su fundación (Bélgica, Dinamarca, Francia, Holanda, Irlanda, Italia, Luxemburgo, Noruega, Reino Unido y Suecia) y pocos meses después se incorporaron Grecia y Turquía. Alemania lo hizo en 1950. España se convirtió en el décimo noveno miembro, el 24 de noviembre de 1977. Desde la incorporación de Montenegro, en 2007, un total de 47 Estados son miembros del Consejo de Europa, siendo Bielorrusia el único Estado europeo que no forma parte de este organismo. Una de las primeras medidas tomadas por el Consejo de Europa fue la redacción en 1950 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, que entró en vigor en el año 1953. Véase, entre otros: AA.VV.: *La Europa de los Derechos. El Convenio Europeo de Derechos Humanos* (GARCÍA ROCA, J. y SANTAOLAYA MACHETTI, P. –coordinadores–), CEPC, Madrid, 2014.

con una regulación específica, al tratarse de un ámbito que requiere de un control y protección especialmente intensos.

Con este propósito, el Convenio núm. 108 dedicó el Capítulo III a los "Flujos transfronterizos de datos de carácter personal", prohibiendo que el intercambio de datos entre los Estados Parte se sujete a límites o a condiciones, salvo que se trate de una trasmisión de datos que, posteriormente, se trasladen a terceros Estados no firmantes del Convenio, todo ello con la finalidad de "evitar que dichas transmisiones tengan como resultado burlar la legislación de la Parte" (art. 12).

Este Convenio fue años después ampliado por el Protocolo Adicional, de 8 de noviembre de 2001, que puso especial atención en las garantías de control de los flujos transfronterizo de datos, como consecuencia del elevado aumento de intercambio de datos personales entre entes públicos y entre particulares, dada la globalización de las relaciones comerciales internacionales.

La última actualización del Convenio (que ha pasado a calificarse como Convenio 108+) se abrió a la firma de los Estados miembros el 10 de octubre de 2018, con dos objetivos principales: por un lado, hacer frente a los retos derivados de la utilización de las nuevas tecnologías de la información y la comunicación y, por otro, reforzar la aplicación efectiva del Convenio.

No forma parte del objeto de este trabajo, centrado en la Unión Europea, el estudio de la jurisprudencia del TEDH, pero resulta inevitable hacer una breve referencia a sus principales Sentencias en materia de protección de datos, dada la influencia de su jurisprudencia en la del TJUE[25], sin olvidar que el art. 8 CDFUE no encuentra un precepto equivalente en el Convenio Europeo de Derechos Humanos (CEDH), el artículo que más se aproxima es el art. 8 CEDH que garantiza el derecho a la vida privada y familiar, así como a la inviolabilidad del domicilio y de las comunicaciones. No obstante, la protección de los datos de carácter personal ha sido garantizada por el TEDH como una vertiente más de la vida privada.

Así, el primer pronunciamiento relevante lo encontramos en la Sentencia de 6 de septiembre de 1978, en el asunto Weber y Saravia c. Alemania, en la que el TEDH se ocupa por primera vez de lo que denomina "vigilancia estratégica generalizada" (*strategic monitoring*) y de la

[25] Véase en este sentido: QUADRA-SALCEDO JANINI, T. DE LA: "El papel del Tribunal Constitucional y de los tribunales ordinarios en un contexto de tutela multinivel de los derechos fundamentales", *El Cronista del Estado Social y Democrático de Derecho*, 2015, p. 35.

obtención de datos personales y su transmisión entre autoridades públicas. Sin embargo, el supuesto que habitualmente se cita como *leading case* es la Sentencia de 26 de marzo de 1987, en el caso *Leander c. Suecia*, jurisprudencia que se reitera en la Sentencia de 24 de mayo de 2000, en el caso *Rotaru c. Rumanía,* de las que se desprende que la protección de datos de carácter personal constituye una vertiente nuclear del derecho a la vida privada, pues aunque no se configura como un derecho autónomo en el Convenio Europeo, el TEDH incluye este derecho en el ámbito de protección del derecho a la vida privada que garantiza el art. 8 del Convenio Europeo de Derechos Humanos.

Con posterioridad a estos pronunciamientos, el TEDH ha declarado que "la vida privada es un término amplio no susceptible de una definición exhaustiva. Aspectos como identidad de género, nombre, orientación y vida sexual, son elementos importantes de la esfera personal protegidos por el artículo 8. El artículo protege también el derecho a la identidad y al desarrollo personal, y el derecho a establecer y desarrollar relaciones con otras personas y con el mundo exterior y puede incluir actividades de naturaleza profesional o comercial. Por lo tanto, existe una zona de interacción de una persona con las otras, incluso en un contexto público, que puede entrar en el ámbito de vida privada" (Caso Perry c. Reino Unido, Sentencia de 17 de julio de 2003, ap. 36)[26].

3.3. La protección de datos en la Unión Europea

Siguiendo el orden cronológico al que antes nos hemos referido, el siguiente instrumento jurídico europeo relevante en la protección de datos de carácter personal lo encontramos en el año 1995, esta vez en el ámbito de la Unión Europea, con la aprobación 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[27], 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.

La Directiva 95/46/CE fue considerada durante años el texto de referencia de la Unión Europea en materia de protección de datos personales, hasta su reciente derogación,

[26] Una relación de SSTEDH relativas al derecho a la vida privada en: SALAMANCA AGUADO, E.: "El respeto a la vida privada y a la protección de datos personales en el contexto de la vigilancia masiva de comunicaciones", *Revista del Instituto Español de Estudios Estratégicos,* núm. 4, 2014, pp. 9 y ss.

[27] 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.

el 25 de mayo de 2018[28], cumpliendo así el objetivo que se desprende de su articulado, que era el de fijar un marco regulador destinado a establecer un equilibrio entre un nivel elevado de protección de la vida privada de las personas y la libre circulación de datos personales dentro de la Unión Europea y en las relaciones internacionales. Con esa finalidad, la Directiva fijaba límites estrictos para la recogida y utilización de los datos personales y solicitaba la creación, en cada Estado miembro, de un organismo nacional independiente encargado de la supervisión de cualquier actividad relacionada con el tratamiento de los datos personales.

Con carácter general, la Directiva 95/46/CE tiene por objeto, conforme a su art. 1.1, garantizar la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales, pues en el momento de su entrada en vigor aún no había sido aprobada la Carta de los Derechos Fundamentales de la Unión en la que, como ya se ha señalado, se recoge el derecho a la protección de datos personales como un derecho fundamental autónomo. Asimismo, en el art. 2, se define el concepto de "dato personal", como "toda información sobre una persona física identificada o identificable", aclarando que se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social.

Tiene también especial relevancia la definición que ofrece la Directiva del "tratamiento de datos personales", que describe como toda operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados y aplicadas a datos personales, tales como "la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción" (art. 2). También, sin ánimo exhaustivo, es de señalar que la Directiva establece una serie de condiciones generales para que se considere legítimo el tratamiento de datos (arts. 5 y ss.) y que se refieren a la necesidad de consentimiento del interesado, salvo excepciones tasadas (art. 7); al derecho de acceso (art. 12) y oposición (art. 14) del interesado; a la confidencialidad (art. 16) y seguridad del tratamiento (art. 17); o al

[28] Como consecuencia de la aprobación del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

conjunto de recursos administrativos y judiciales con los que cuenta el interesado para hacer valer este derecho (art. 22).

De entre los preceptos citados interesa prestar una especial atención, en relación con el objeto de este trabajo, al art. 17.1, que fija lo siguiente: "Los Estados miembros establecerán la obligación del responsable del tratamiento de aplicar las medidas técnicas y de organización adecuadas, para la protección de los datos personales contra la destrucción, accidental o ilícita, la pérdida accidental y contra la alteración, la difusión o el acceso no autorizados, en particular cuando el tratamiento incluya la transmisión de datos dentro de una red, y contra cualquier otro tratamiento ilícito de datos personales".

Reproducimos este artículo porque, teniendo en cuenta que la Directiva se aplica, como se desprende de su contenido, tanto a los ficheros tradicionales en papel, como, sobre todo, a los datos tratados por medios automatizados (base de datos personales de clientes de una empresa multinacional, por ejemplo), unido a la circunstancia de que su protección se extiende "a la transmisión de datos dentro de una red", parece claro que se trata de un artículo del que se desprenden un conjunto de garantías de protección de los datos de carácter personal no sólo en el ámbito interno de la Unión Europea, sino también respecto de las transferencias de datos personales que, a través de los diversos "sistemas tecnológicos en red", puedan llegar a terceros países.

En relación con esta última cuestión la Directiva 95/46/CE dedica el Capítulo IV a "La transferencia de datos personales a países terceros", que contiene dos extensos artículos: el art. 25, en el que se exige que los Estados miembros deberán asegurar que las transferencias a un país tercero de datos personales que sean objeto de tratamiento (o destinados a ser objeto de tratamiento con posterioridad a su transferencia), únicamente podrá efectuarse cuando el país tercero "garantice un nivel de protección adecuado"; y el art. 26, donde se recogen un conjunto de excepciones a esta exigencia.

En el citado art. 25 se fijan unas pautas que ayudan a evaluar cuándo un país tercero cuenta con "un nivel de protección adecuado", indicando que 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", estando obligados, los Estados miembros y la Comisión, a informarse recíprocamente de los casos en que consideren que un tercer país no garantiza un nivel de protección adecuado, situación en la que los Estados miembros

adoptarán las medidas necesarias para impedir cualquier transferencia de datos personales al tercer país en cuestión.

Sin perjuicio de lo dispuesto en este artículo, cabe la posibilidad de que los Estados miembros permitan la transferencia de datos personales a un país tercero que no garantice "un nivel de protección adecuado", cuando se den alguno de los supuestos recogidos en el art. 26.1 de la Directiva, esto es:

a) que el interesado haya dado su consentimiento inequívoco a la transferencia prevista, o

b) que 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 tomadas a petición del interesado, o

c) que la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero, o

d) que la transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial, o

e) que la transferencia sea necesaria para la salvaguardia del interés vital del interesado, o

f) que la transferencia tenga lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta.

Asimismo, los Estados miembros podrán autorizar una transferencia o una serie de transferencias 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 en relación con el ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, *de cláusulas contractuales apropiadas*.

En conexión con el objeto de este trabajo, también resulta interesante destacar que la Directiva regula, en el art. 28, dentro del Capítulo VI, la figura de la "autoridad de control",

que la propia norma define como aquella autoridad pública "encargada de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva", estableciendo de forma no exhaustiva (art. 28.2) algunas de sus facultades, tales como su potestad investigadora, el ejercicio de poderes de intervención (como el de formular dictámenes antes de realizar los tratamientos, o el de ordenar el bloqueo, la supresión o la destrucción de datos, entre otros), a lo que se añade su capacidad procesal, para poner en conocimiento de la autoridad judicial aquellos casos en que se infrinjan las disposiciones nacionales adoptadas en aplicación de la presente Directiva.

La creación en los Estados miembros de autoridades de control independientes constituye un mecanismo fundamental de cara a la protección de las personas frente al tratamiento de datos personales, siendo abundante la jurisprudencia del Tribunal de Justicia de la Unión Europea que pone especial énfasis en su importancia[29], destacando en este sentido las SSTJUE Schrems I y Schrems II, como se verá con detenimiento más adelante.

Aparentemente, se ha de entender que la actuación de estas autoridades se ciñe a los tratamientos de datos realizados dentro de su propio Estado y que tales autoridades, al menos con apoyo en el art. 28 de la Directiva, carecen de facultades de control con respecto a tratamientos realizados en un tercer país. Sin embargo, el TJUE, estimando que la transferencia de datos de un país a otro supone, en sí misma, un tratamiento de datos personales de ciudadanos del país de origen, terminará confirmando que la autoridad del país en cuestión podrá controlar la transferencia efectuada, asegurando el respeto pleno de las disposiciones adoptadas por los Estados miembros en aplicación de la Directiva 95/46, tal y como se desprende del considerado 60 de la misma (sobre esta cuestión volveremos cuando analicemos la STJUE Schrems I).

Continuando con la exposición cronológica de los principales instrumentos jurídicos de la Unión Europea en relación con la protección de datos de carácter personal y, de forma más concreta, con la protección de los datos objeto de las transferencias a terceros países, debemos llamar la atención sobre diversas Decisiones de la Comisión[30], comenzando con la

[29] SSTJUE de 9 de marzo de 2010, Comisión/Alemania (C-518/07, EU:C:2010:125), apartado 25 y de 8 de abril de 2014, Comisión/Hungría (C-288/12, 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, citada, en sus apartado 24 y 51, respectivamente).

[30] De acuerdo con lo dispuesto en los artículos 288 y siguientes del TFUE, la Decisión es una norma jurídica de Derecho comunitario europeo que vincula a sus destinatarios en todos sus elementos y de manera directa e inmediata. 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. Cuando designe destinatarios, la Decisión sólo obligará a estos. La Decisión es uno de los tres tipos normativos o fuentes formales del Derecho que existen en la Unión

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[31], 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, sobre la que volveremos en los siguientes apartados, pues constituye el objeto de impugnación de la STJUE Schrems I.

Adelantamos que se trata de una *Decisión de adecuación parcial*, es decir, la mera aprobación de la Decisión 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, sólo servirá de cobertura legal a aquellas empresas norteamericanas que se comprometan a cumplir todos los principios recogidos en el mismo, pero resulta un caso paradigmático que pone de relieve algunos de los problemas que surgen con terceros países 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 *cláusulas contractuales tipo* para la transferencia de datos personales a un tercer país, según lo previsto en la Directiva 95/46/CE. Esta Decisión 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 terceros países y obliga a los Estados miembros a reconocer que las sociedades u organismos que utilicen esas *cláusulas tipo* en contratos relativos a transferencias de datos personales a terceros países garantizan un nivel adecuado de protección.

Pocos años después, se aprueba la Decisión 2004/915/CE de la Comisión, de 27 de diciembre de 2004, por la que se modifica la Decisión 2001/497/CE en lo relativo a la introducción de un conjunto alternativo de *cláusulas contractuales tipo* para la transferencia de datos personales a terceros países. Y, 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, relativa a

Europea y tienen carácter vinculante (los otros dos son el Reglamento y la Directiva). La Decisión se asemeja en sus efectos al Reglamento, puesto que no necesita de transposición al Derecho interno de los Estados, dado que reviste eficacia directa, pero se diferencia de aquel porque no posee necesariamente el alcance general ni la abstracción que caracteriza al Reglamento.

[31] El art. 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, a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas".

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 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 en materia de protección de datos en la Unión Europea.

Una importante característica de este texto es que, al tratarse de un Reglamento, su aplicación a los diferentes Estados miembros es directa, sin necesidad de trasposición por las normas nacionales de los Estados, lo que ha permitido una armonización de la protección de datos en todos los Estados miembros de la UE, solucionando la dispersión normativa que existía anteriormente.

En términos similares a la Directiva 95/46/UE, la protección del Reglamento se extiende al tratamiento de los datos personales de todas las personas físicas que se encuentren en el territorio de la Unión Europea, independientemente de su nacionalidad o de su lugar de residencia. Se excluye el tratamiento de datos personales relativos a personas jurídicas y también se excluyen de su ámbito de protección los datos personales de personas fallecidas; mientras que, por el contrario, reciben una especial atención los datos personales de los menores y, a los efectos que ahora nos interesan, también las transferencias internacionales de datos a terceros países.

El RGPD fija en el art. 4 una serie de "definiciones" que hemos de tener en cuenta. Así, define los "datos personales" como "toda información sobre una persona física identificada o identificable" (art. 4.1), aclarando, en ese mismo primer apartado, que se entiende por tal "aquella persona cuya identidad pueda ser determinada de forma directa o indirecta mediante la utilización de cualquier tipo de identificador como pueda ser un nombre, número de identificación o datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona".

Más difícil resulta definir el concepto de "información", pues no podemos entender que se refiere únicamente a datos confidenciales o directamente relacionados con esferas de intimidad, dado que puede afectar a cualquier tipo de identificador sobre la "persona física identificada o identificable". Esto hace que sean considerados datos personales desde el nombre, estado civil, profesión o número de teléfono, a materias más sensibles como la salud, la religión, la orientación sexual, el historial de búsquedas en Internet, el ID de los dispositivos personales o las imágenes obtenidas a través de cámaras de videovigilancia, por ejemplo.

Encontramos cierta aclaración al respecto en el considerando número 26 del RGPD, donde se indica que "para determinar si una persona física es identificable, deben tenerse en cuenta todos los medios, como la singularización, que razonablemente pueda utilizar el responsable del tratamiento o cualquier otra persona para identificar directa o indirectamente a la persona física". En este mismo considerando el RGPD aclara que: "los principios de protección de datos no deben aplicarse a la información anónima, es decir información que no guarda relación con una persona física identificada o identificable, ni a los datos convertidos en anónimos de forma que el interesado no sea identificable, o deje de serlo. En consecuencia, el presente Reglamento no afecta al tratamiento de dicha información anónima, inclusive con fines estadísticos o de investigación".

Con la finalidad de aportar algo más de luz en relación con el objeto de protección del Reglamento, el Comité Europeo de Protección de Datos, que tiene como función garantizar que el RGPD se aplique de manera coherente y efectiva en los países de la Unión Europea, ha venido insistiendo en que la definición de "datos personales" tiene un contenido muy amplio, incluyendo cualquier tipo de referencia a la identidad física, económica, cultural o social de una determinada persona, sin que resulte necesario que exista una coincidencia absoluta entre el dato y la persona, siendo suficiente con que pueda realizarse la identificación utilizando medios "razonables" y "no desproporcionados" para ello[32].

El citado Comité Europeo también deja claro que resulta indiferente, tanto la tecnología o medios utilizados para el tratamiento de los datos personales, como el tipo de almacenamiento, pues el RGPD se aplicará igualmente a aquellos datos almacenados de forma física, en papel, como a los que se encuentren en bases informatizadas de datos[33].

[32] https://edpb.europa.eu/edpb_es.

[33]https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_es#:~:text=Los%20datos%20personales%20son%20cualquier,constituyen%20datos%20de%20car%C3%A1cter%20personal.

En todo caso, el Comité también reconoce que no todos los datos personales han de tener el mismo nivel de protección, pues no afecta de igual forma a la intimidad de una persona el conocimiento por parte de terceros, a través de una base de datos, de su número de teléfono, que el almacenamiento y tratamiento de datos personales tales como la pertenencia a una determinada confesión religiosa, por ello hay determinados datos que se encuentran protegidos de una forma reforzada por afectar a la esfera más íntima de la personal.

Así, el artículo 9 RGPD recoge aquellos datos catalogados como especialmente sensibles, para cuyo tratamiento se deberá cumplir con unas estrictas circunstancias habilitantes. Así, el art. 9.1 RGPD prohíbe el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, así como el tratamiento de datos genéticos y de datos biométricos dirigidos a identificar de manera unívoca a una persona física, y el tratamiento de datos relativos a la salud, a la vida sexual o a la orientación sexual. En conexión con los datos especialmente sensibles, el considerando número 51 del Reglamento aclara que el tratamiento de fotografías no debe considerarse automáticamente como un tratamiento de "categorías especiales de datos personales", pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física.

Esta prohibición de tratamiento de datos especialmente sensibles cuenta con una serie de excepciones que se concretan en el art. 9.2 RGPD, tales como el consentimiento explícito del interesado (excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición no puede ser levantada por el interesado); el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en los término previstos en el Derecho de la Unión; la necesidad de tratamiento de dichos datos por razones de interés público o para fines de medicina preventiva o laboral; la gestión de los sistemas y servicios de asistencia sanitaria y social, de acuerdo con el Derecho de la Unión y de los Estados miembros, entre otras excepciones.

Una vez delimitado el concepto de datos de carácter personal, entiendo que un análisis detallado de todo el contenido del RGPD excedería el objeto de este trabajo[34], por lo que me limitaré a exponer los rasgos esenciales del régimen de protección que dicho texto jurídico fija en relación con las transferencias internacionales de datos personales, sin

[34] Un estudio exhaustivo de dicho texto jurídico en: TRONCOSO REIGADA, A.: *Comentarios al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales*, Cívitas, Pamplona, 2021.

perjuicio de que, por razones sistemáticas, dedicaremos a esta materia el último epígrafe de este trabajo.

Pues bien, 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 cuando se dan los siguientes elementos:

- Debe contener datos de carácter personal, de acuerdo con la definición prevista en el art. 4 RGPD, de donde se desprende que se podrán considerar tales cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables, en los términos previstos en el citado precepto.

- Los datos transferidos podrán haber sido tratados tanto de forma automatizada como manual.

- La transferencia debe realizarse con el fin de llevar a cabo un tratamiento por parte del destinatario de los mismos.

- Se debe producir el efectivo traslado físico de los datos.

- El lugar de destino debe de encontrarse fuera de la Unión Europea.

A partir de estos parámetros generales, los requisitos que han de cumplir las transferencias internacionales de datos desde la Unión Europea se encuentran regulados específicamente en el RGPD, pues como se indica en el considerando número 5, la integración económica y social resultante del funcionamiento del mercado interior ha llevado a un aumento sustancial de los flujos transfronterizos de datos personales, produciéndose en toda la Unión un incremento del intercambio de datos personales entre los operadores públicos y privados, incluidas las personas físicas, las asociaciones y las empresas, razones

por las que, como se indica explícitamente en dicho considerando: "el Derecho de la Unión insta a las autoridades nacionales de los Estados miembros a que cooperen e intercambien datos personales a fin de poder cumplir sus funciones o desempeñar otras por cuenta de una autoridad de otro Estado miembro".

Pues bien, el Capítulo V del RGPD se dedica a la "Transferencias de datos personales a terceros países u organizaciones internacionales" (artículo 44 al 50), que, por razones sistemáticas, analizaremos con detenimiento más adelante.

4. LAS TRANSFERENCIAS DE DATOS DE CARÁCTER PERSONAL ENTRE EUROPA Y ESTADOS UNIDOS: EL ACUERDO DE PUERTO SEGURO (*SAFE HARBOUR*) RECOGIDO EN LA DECISIÓN 2000/520/CE DE LA COMISIÓN, DE 26 DE JULIO DE 2000

4.1. Una Decisión de la Comisión dirigida a proteger los datos personales transferidos desde la Unión Europea a empresas norteamericanas.

Como hemos adelantado, la Decisión 2000/520/CE, de 26 de julio de 2000, fue adoptada por la Comisión, con apoyo en el art. 25.6 de la Directiva 95/46, con la finalidad de establecer un nivel adecuado de protección de los datos de carácter personal en las transferencias de datos 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, en lo que a protección de datos personales se refiere, 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[35].

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 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 dichas empresas.

Así, con la finalidad de cumplir lo dispuesto en el art. 25.2 de la Directiva 95/46[36], la Decisión establecía que el nivel adecuado de protección de la transferencia de datos desde la Unión Europea a los Estados Unidos de América sólo 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, la Decisión recogía un conjunto 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, pues se trataba de las respuestas a aquellas preguntas más frecuentes planteadas ante el Departamento de Comercio de los Estados Unidos de América en relación con la interpretación y aplicación del *Acuerdo de Puerto Seguro*. Por su parte, las entidades y empresas 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*), debiendo cumplir rigurosamente lo previsto en el art. 5 del *Federal Trade Commission Act*, que prohíbe actos o prácticas desleales o fraudulentas en el comercio o en relación con él.

---

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

[36] El art. 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".

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 derivan 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 manifestaba su adhesión a los *Principios de Puerto Seguro.*

¿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[37] 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*.

La Carta debía contener la siguiente información: 1) nombre de la entidad, dirección postal, correo electrónico, teléfono y fax; 2) descripción de las actividades de la entidad en lo relativo a la información personal recibida de la Unión Europea; y 3) descripción de su política de protección de la vida privada respecto de dicha información personal, con indicación de: a) el lugar donde puede ser consultada por el público; b) la fecha de entrada en vigor de dicha política; c) una oficina de contacto para la tramitación de las quejas, las solicitudes de acceso y cualquier otra cuestión relacionada con los *Principios de Puerto Seguro*; d) el organismo oficial concreto con jurisdicción para entender de cualquier queja contra la entidad por posibles prácticas desleales o fraudulentas y vulneraciones de las leyes o normas sobre la vida privada; e) el nombre de los programas de protección de la vida privada a los que esté adscrita la entidad; f) el método de verificación (por ejemplo, interna, por terceros) […]; y g) la instancia independiente encargada de investigar las quejas no resueltas.

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.

[37] Por razones de transparencia el anexo II de la Decisión 2000/520 se recogen algunas de las *Preguntas más frecuentes* (FAQ).

También es de señalar que el art. 3 de la Decisión establecía la posibilidad de que las autoridades competentes de los Estados miembros, con la finalidad de proteger a los particulares contra el tratamiento desleal de sus datos personales, podían ejercer la facultad de suspender los flujos de datos hacia una entidad o empresa, incluso en aquellos casos en que existiera una *carta de autocertificación* manifestando la adhesión a los Principios de Puerto Seguro. Esta facultad podía ejercerse, no sólo cuando el organismo competente de los Estados Unidos hubiese resuelto que la entidad o empresa norteamericana había vulnerado los Principios de Puerto Seguro, sino también cuando la autoridad competente de un Estado de la Unión Europea entendiese que existían grandes probabilidades de que se estuviesen vulnerando los principios recogidos en la Decisión, existiendo un riesgo inminente de grave perjuicio a los afectados.

En el Anexo I de la Decisión se recogen los *Principios de Puerto Seguro*, que pueden sintetizarse 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 utilización 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 con los que se utilizan.

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.

Como ya se ha indicado, estos principios se fueron completando por medio de las FAQ, que eran resueltas por el Departamento de Comercio de los Estados Unidos, en colaboración con el Comité Europeo de Protección de Datos.

De acuerdo con lo expuesto, todo parecía indicar que la Decisión 2000/520 colocaba a los Estados Unidos como un destino con suficientes garantías de protección de los datos personales de los ciudadanos europeos. Sin embargo "el Puerto de destino" no resultó "tan seguro" como se pretendía, pues los principios generales antes expuestos cedían en aquellos supuestos en que las autoridades norteamericanas invocases 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 sólo 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 EE.UU.

Esta posible intervención de las autoridades públicas norteamericanas estaba contemplada en el anexo I de la Decisión 2000/520, donde se recogía que la adhesión a los *Principios de Puerto Seguro* podía limitarse en una serie de supuestos:

a) Cuando fuese necesario para cumplir las exigencias de seguridad nacional, interés público y cumplimiento de la ley.

b) Por disposición legal, reglamentaria o jurisprudencial, que originen conflictos de obligaciones.

c) Por excepción o dispensa prevista en la Directiva o en las normas de Derecho interno de los Estados miembros, siempre que tal excepción o dispensa se aplique en contextos comparables.

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 hemos adelantado en la introducción, en junio de 2013 el Sr. Edward Snowden, un joven informático norteamericano que trabajaba para la Agencia de Seguridad Nacional de Estados Unidos, descubrió e hizo pública la vigilancia ejercida sobre ciudadanos norteamericanos y de terceros países por el ejecutivo de los Estados Unidos, que, 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. El Sr. 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 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"[38], que iba acompañada de un Informe, también con fecha de 27 de noviembre de 2013, sobre protección de datos personales 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*).

Dicho Informe 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 autoridades estadounidenses, que hay que poner en conexión con lo dispuesto en el punto 2 de la Comunicación, en el que la Comisión manifiesta 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 , también de

[38] COM (2013) 846 final.

la Comunicación, en el que la Comisión constató serias deficiencias en la aplicación de la Decisión 2000/520, poniendo de manifiesto que algunas empresas estadounidenses certificadas no respetaban los principios de Puerto Seguro a pesar de haberse comprometido a ello, sin que existieran en los Estados Unidos mecanismos jurídicos para hacer efectivo dicho compromiso. Sin embargo, una lectura pausada del documento lleva a concluir que el problema de fondo no procede de eventuales infracciones por parte de las empresas, sino del acceso (generalizado y sin someterse a ningún test de necesidad, ni de proporcionalidad) de las autoridades norteamericanas, a los datos de carácter personal de ciudadanos comunitarios que se encontraban en ficheros de empresas domiciliadas en Estados Unidos.

Como consecuencia de lo anterior, la Comisión concluyó, en el punto 3.2 de la Comunicación, que: "habida cuenta de las deficiencias halladas, no puede mantenerse la aplicación actual del régimen de Puerto Seguro", 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 subsanar dichas deficiencias, pues con la mera invocación de la excepción de "motivos de seguridad nacional", las empresas norteamericanas firmante del *Acuerdo de Puerto Seguro*, no pueden verse obligadas a proporcionar a las autoridades de Estados Unidos datos personales a gran escala[39].

Por último, la Comisión manifiesta, en el punto 7 de la Comunicación, que "aparentemente todas las empresas involucradas en el programa PRISM [programa de recogida de informaciones a gran escala], y que concede a las autoridades estadounidenses acceso a los datos almacenados y tratados en Estados Unidos, tienen el certificado de puerto seguro", y ello ha convertido el *Acuerdo de Puerto Seguro* en "uno de los conductos a través de los cuales se da acceso a las autoridades de inteligencia estadounidenses para recopilar datos personales que han sido tratados inicialmente en la [Unión]", constatando, asimismo, que "diversas bases legales con arreglo al ordenamiento jurídico estadounidense permiten la recogida y el tratamiento a gran escala de datos personales almacenados o tratados con otra finalidad por empresas y entidades de Estados Unidos".

[39] 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 3246 entidades pertenecientes a sectores de la industria y de sectores de servicios. Esas empresas prestaban principalmente servicios en el mercado interior de la Unión, en particular en el sector de Internet, y algunas de ellas eran empresas de la Unión que tenían filiales en Estados Unidos. Parte de esas empresas trataban los datos de sus empleados en Europa, datos que transferían a Estados Unidos para la gestión de sus recursos humanos.

Hay que recocer que la Comisión no utiliza precisamente 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 "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]"; 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 recogidos y tratados como consecuencia de los programas de vigilancia de las autoridades norteamericanas[40].

La Comisión concluye, en el punto 8, que "el acceso a gran escala por parte de las agencias de inteligencia a los datos transferidos a Estados Unidos por entidades con certificación de Puerto Seguro suscita serias cuestiones adicionales en lo que respecta al derecho de los europeos a que sus datos sigan estando protegidos cuando se transfieren a ese país".

De hecho, algunos Estados miembros europeos, como Alemania, comenzaron a llevar a cabo acciones unilaterales frente a EE. UU., 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 EE. UU., 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*[41]. 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*)

[40] Sobre el programa de vigilancia de la Agencia de Seguridad Nacional de los EE.UU., 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 la dirección de Internet: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2014-0139+0+DOC+PDF+V0//ES

[41] Dicha resolución está disponible (en inglés) en: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/ErgaenzendeDokumente/PMDSK_SafeHarbor_Eng.pdf?__blob=publicationFile.

emitió un comunicado manifestando 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[42].

Pese a todas estas denuncias, desatadas a partir de la información proporcionada por Edward Snowden, 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 Estados Unidos y la Unión Europea, por lo que la Comisión no se planteó suspender la Decisión de adecuación que amparaba dicho Acuerdo. Sin embargo, como se analizará a continuación, el *Acuerdo de Puerto Seguro* sucumbió definitivamente cuando el TJUE dictó la Sentencia, de 6 de octubre de 2015, en el asunto C-362/14, Maximilian Schrems vs *Data Protection Comisiones*, donde declara inválida la Decisión 200/520/CE de 26 de julio de 2000.

Todo ello nos sitúa ante una cuestión mucho más amplia de la que ahora estamos analizando, esto es, ante los diferentes sistemas de concepción y protección de los datos de carácter personal que existen entre EE. UU. y la Unión Europea[43]. De hecho, en las negociaciones entre ambos países, previas a la firma del *Acuerdo de Puerto Seguro*, se puso de relieve que la *Federal Trade Commission* norteamericana era favorable a la "autorregulación" entre las empresas y los interesados, al considerar que se trataba de un sistema que, por un lado, aseguraba la protección de los datos de carácter personal y, por otro, favorecía las relaciones económicas. Por el contrario, la Comisión Europea defendía la existencia de una regulación general y detallada, vinculante para poderes públicos y particulares.

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

[43] Para ver las diferencias sobre el modo en el que se protege la privacidad en la UE en comparación con EE.UU, ver, 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, M. e URIARTE LANDA, I.: "Dos visiones sobre la regulación de la privacidad y la innovación digital", *Expansión* (sección Jurídico), 12 de septiembre de 2014.

5. ANÁLISIS DE LA SENTENCIA SCHREMS I (STJUE DE 6 DE OCTUBRE DE 2015, EN EL ASUNTO *MAXIMILIAN SCHREMS VS. DATA PROTECTION COMMISSIONER*)

5.1. Litigio principal y cuestiones prejudiciales.

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, que acabamos de analizar, así como las críticas a la política de vigilancia de las autoridades norteamericanas en la prensa estadounidense[44], que pronto tuvo eco en toda la prensa mundial, provocó una creciente inquietud entre la población que facilitó el camino para que un ciudadano austriaco, el Sr. Schrems, se decidiera a iniciar un proceso judicial contra la empresa norteamericana *Facebook* , en una especie de enfrentamiento de David contra Goliat, 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.*

Esta Sentencia resuelve la cuestión prejudicial planteada, con arreglo al artículo 267 TFUE, por la *High Court* (Tribunal Superior de Irlanda) en el procedimiento entre Maximillian Schrems y Data Protection Commissioner. La petición de decisión prejudicial tiene por objeto la interpretación de los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea; de los artículos 25.6 y 28 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, así como, en esencia, la validez de la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, sobre la adecuación de la protección conferida por el *Acuerdo de Puerto Seguro*, que acabamos de analizar.

---

[44] Véanse los incisivos artículos publicados en *The Guardian y The Washington Post*, entre junio y agosto de 2013, entre otros: GREENWALD, G.: "NSA collecting phone records of millions of Verizon customers daily", en *The Guardian*, jueves 6 de junio de 2013 [https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order]; GELLMAN, B y POITRAS, L.: "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program", en *The Washington Post*, 7 de junio de 2013 [https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html]; GREENWALD, G. y MACASKILL, E.: "NSA Prism program taps in to user data of Apple, Google and others", cit.; HOPKINS, N.: "UK gathering intelligence via covert NSA operation", en *The Guardian*, 7 Junio 2013 [https://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism].

La petición se presenta en el marco de un litigio entre el Sr. Schrems (nacional austriaco residente en Austria y 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, pues dirige la Comisión de Protección de Datos [*The Data Protection Commission* (DPC)], esto es, el máximo organismo nacional independiente, responsable de defender el derecho fundamental de las personas a la protección de datos en Irlanda.

El litigio en cuestión surgió como consecuencia de la negativa del Comisario a instruir y tramitar una reclamación presentada por el Sr. Schrems, basada en que *Facebook Ireland* transfería a Estados Unidos los datos personales de sus usuarios, almacenándolos en sus servidores estadounidenses sin cumplir los principio previstos en el *Acuerdo de Puerto Seguro* previsto en la Decisión 2000/520/CE de la Comisión, en los términos que explicaremos a continuación.

5.2. Antecedentes

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 Estados Unidos), y que los datos de los usuarios europeos de *Facebook Ireland* son trasladados a los servidores centrales de *Facebook Inc.* situados en Estados Unidos, donde son objeto de tratamiento.

El 25 de junio de 2013 el Sr. Schrems decidió presentar ante el Comisario una reclamación en la que solicitaba que desde la Comisión de Protección de Datos se prohibiera a *Facebook Ireland* la transferencia de los datos personales de sus usuarios al servidor de 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 resulta muy grave, según el recurrente, cuando la injerencia se producía como consecuencia de las actividades de vigilancia practicadas por las autoridades públicas norteamericanas. El Sr. Schrems hacía referencia, en ese sentido, a las revelaciones que hizo a la prensa el Sr. Edward Snowden sobre las actividades de los servicios de información de

Estados Unidos, en particular las de la Agencia de Seguridad Nacional de Estados Unidos [*National Security AFICSgency* (NSA)].

Pese a la importancia de un tema que estaba siendo objeto de análisis por parte de los gobiernos de los distintos estados miembros de la Unión Europea, el Comisario desestimó la reclamación del Sr. Schrems, calificándola de infundada, al entender que no había pruebas de que la NSA hubiera accedido a los datos personales del demandante y añadiendo que cualquier cuestión referida a la protección de datos trasferidos desde Europa a Estados Unidos debía ser resuelta aplicando lo dispuesto en la Decisión 2000/520, en la que se fijaban los *Principios de Puerto Seguro* que seguía vigente, pues no había sido suspendida por la Comisión.

Pues bien, frente a la desestimación del Comisario, el Sr. Schrems interpuso un recurso ante la *High Court* (Tribunal Supremo de Irlanda), que fue admitido a trámite, tal y como se desprende de los antecedentes de la STJUE que analizamos. La *High Court*, tras examinar las pruebas presentadas por las partes, consideró que, aunque la Comisión Europea entendía en el *Acuerdo de Puerto Seguro*, que la vigilancia electrónica e interceptación de datos personales de ciudadanos de la Unión Europea por parte de la Agencia de Seguridad Nacional de Estados Unidos era restrictiva y servía a finalidades necesarias de interés público, lo cierto es que, en el caso concreto que se presenta a examen, las revelaciones del Sr. Snowden habían demostrado la comisión de "importantes excesos" por parte de la NSA y otros organismos federales, que no podían quedar exentos de investigación.

El Alto Tribunal constató igualmente que la supervisión de las acciones de los servicios de inteligencia de los Estados Unidos se realizaba a través de un procedimiento secreto y no contradictorio, no disponiendo los ciudadanos de la Unión Europea de información precisa en relación con la obtención y utilización de sus datos personales, sin que el ordenamiento norteamericano contemplase ningún derecho a obtener dicha información, ni la posibilidad, en su caso, de acudir a los tribunales de justicia. En suma, el Tribunal Supremo de Irlanda llegó a la conclusión de que, una vez transferidos los datos personales a Estados Unidos, la NSA y otros organismos federales como el *Federal Bureau of Investigation* (FBI), podían acceder a ellos invocando genéricas razones de seguridad nacional, realizando interceptaciones indiferenciadas de datos, a gran escala.

En síntesis, la *High Court* entendió que el acceso masivo e indiferenciado a datos personales constatado por el Sr. Snowden y que denunciaba en su demanda el Sr. Schrems, era manifiestamente contrario al principio de proporcionalidad y a los valores fundamentales

protegidos por la Constitución irlandesa, por lo que consideró que Estados Unidos debería garantizar que esa interceptación de datos tenía carácter selectivo y que estaba individualmente justificada por motivos de seguridad nacional, además de probar que existían garantías jurídicas efectivas de protección para los afectados.

Por las razones anteriormente expuestas, la *High Court* entendió que, con fundamento exclusivo en el Derecho Irlandés, existían serias dudas de que los Estados Unidos estuvieran garantizando un nivel adecuado de protección de los datos personales transferidos desde Europa, por lo que el Comisario debería haber llevado a cabo una investigación más exhaustiva sobre los hechos denunciados por el Sr. Schrems en su reclamación, habiendo sido indebidamente desestimada.

En consecuencia, el Tribunal irlandés, sin entrar a resolver el fondo de la cuestión, consideró que el recurrente había visto vulnerado su derecho a la tutela judicial efectiva, pues el Comisario no había llevado a cabo una investigación suficiente, dirigida a esclarecer las acusaciones vertidas por el demandante, limitándose a considerar formalmente válida la Directiva 95/46/CE y el *Acuerdo de Puerto seguro* que se deriva de la misma.

Sin embargo, la *High Court* no sólo exigió al Comisario la admisión a trámite de la queja para su correcta resolución, sino que dio un paso más al entender que se encontraba ante un caso que sobrepasa el Derecho irlandés, siendo de aplicación el Derecho de la Unión Europea, pues la prohibición de la transferencia de datos fuera del territorio nacional en aquellos casos en los que el tercer país interesado no pueda asegurar un nivel de protección adecuado de la vida privada y de los derechos y libertades fundamentales de los afectados, constituye una regla de obligatorio cumplimiento para todos los Estados miembros, de acuerdo con la Directiva 95/46.

Además, en este caso, al tratarse de Estados Unidos, no sólo resultaba de aplicación la Directiva, sino que también era necesario enjuiciar la validez de la Decisión 2000/520, con lo que se trataba de un caso que afectaba al Derecho de la Unión, siendo de aplicación lo previsto en el art. 51.1 de la Carta de derechos Fundamentales de la Unión Europea, que establece:

> 'Las disposiciones de la presente Carta están dirigidas a las instituciones, órganos y organismos de la Unión, dentro del respeto del principio de subsidiariedad, así como a los Estados miembros únicamente cuando apliquen el Derecho de la Unión. Por consiguiente, éstos respetarán los derechos, observarán los principios y promoverán su aplicación, con

arreglo a sus respectivas competencias y dentro de los límites de las competencias que los Tratados atribuyen a la Unión".

Pues bien, la *High Court* llegó a la conclusión de que existían serias dudas de que la Decisión 2000/520 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[45], 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 acceder a las comunicaciones electrónicas y a los datos de carácter personal de manera aleatoria y generalizada, sin ninguna justificación objetiva fundada en motivos de seguridad nacional, motivos que deberían estar regulados de forma clara y previsible.

La *High Court* consideró también que, en realidad, el Sr. Schrems impugnaba en su recurso la licitud del *Acuerdo de Puerto Seguro* (*Safe Harbour*) establecido por la Decisión 2000/520, de la cual deriva la decisión discutida en el litigio principal, por lo que, a pesar de que el demandante no impugnó formalmente la validez de la Directiva 95/46, ni la validez de la Decisión 2000/520, la *High Court* suspendió el procedimiento y planteó al Tribunal de Justicia dos cuestiones prejudiciales que pueden sintetizarse en los siguientes puntos:

1) Si en el marco de la resolución de una reclamación presentada ante el Comisario, en la que se afirma que se están transmitiendo datos personales a un tercer país (en el caso de autos, a Estados Unidos) cuya legislación no prevé una protección adecuada de la persona sobre la que versan los datos: ¿está vinculado dicho Comisario en términos absolutos por la declaración comunitaria en sentido contrario contenida en la Decisión 2000/520, habida cuenta de los artículos 7, 8 y 47 de la Carta y sin perjuicio de lo dispuesto en el artículo 25, apartado 6, de la Directiva 95/46/CE?

2) En caso contrario, ¿puede o debe realizar dicho Comisario su propia investigación del asunto a la luz de la evolución de los hechos que ha tenido lugar desde que se publicó la Decisión 2000/520?

[45] C-293/12 y C-594/12, 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.

5.3. El importante papel de las autoridades nacionales de control

La primera de las cuestiones prejudiciales planteadas da ocasión al Tribunal de Justicia Europeo para delimitar el ámbito de competencias de las autoridades de control de cada uno de los Estados miembros, así como la extensión territorial de sus facultades de control cuando, como es el caso, el tratamiento de los datos personales tiene lugar fuera de las fronteras del Estado en el que ejerce su labor.

Así, la pregunta que formula el tribunal irlandés es, literalmente, la siguiente:

> *"*si el artículo 25, apartado 6, de la Directiva 95/46, entendido a la luz de los artículos 7, 8 y 47 de la Carta, debe interpretarse en el sentido de que una decisión, como la Decisión 2000/520, por la que la Comisión constata que un tercer país garantiza un nivel de protección adecuado, impide que una autoridad de control de un Estado miembro, a la que se refiere el artículo 28 de esa Directiva, pueda examinar la solicitud de una persona relativa a la protección de sus derechos y libertades frente al tratamiento de sus datos personales, que se hayan transferido desde un Estado miembro a ese tercer país, cuando esa persona afirma que el Derecho y las prácticas en vigor en éste no garantizan un nivel de protección adecuado*"*.

Para entender el razonamiento y el fallo de esta Sentencia es necesario tener en cuenta que las facultades de las autoridades nacionales de control tiene una regulación específica en el artículo 28 de la Directiva 95/46 que, como ya hemos referido anteriormente, obliga a los países a instituir una o más autoridades públicas independientes, destinadas al control del cumplimiento de las normas de la UE en esta materia, una exigencia derivada también del artículo 8.3 de la Carta y del art. 16 TFUE.

La cuestión que se eleva al TJUE tiene su origen en los problemas de interpretación del art. 28 de la Directiva 96/46, del que parece desprenderse que las facultades de las autoridades nacionales de control sólo se extienden a los tratamientos de datos personales realizados en el territorio del Estado al que pertenecen esas autoridades, sin que dispongan de poder para controlar los tratamientos de datos realizados en el territorio de un tercer país, pues el citado precepto dispone que: "Los Estados miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva" (art. 28.1).

La referencia expresa al territorio al que pertenece la autoridad de control se repite en el art. 28.6, que establece: "Toda autoridad de control será competente, sean cuales sean las disposiciones de Derecho nacional aplicables al tratamiento de que se trate, para ejercer en el territorio de su propio Estado miembro los poderes que se le atribuyen en virtud del apartado 3 del presente artículo. Dicha autoridad podrá ser instada a ejercer sus poderes por una autoridad de otro Estado miembro".

Pues bien, a pesar del tenor literal del art. 28, el TJUE aclara que el considerando 60 de la Directiva 95/46 precisa que las transferencias de datos personales hacia terceros países sólo podrán efectuarse si se respetan plenamente las disposiciones adoptadas por los Estados miembros en aplicación de la misma Directiva, de donde se desprende, según entiende el TJUE, que 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).

El TJUE completa su argumentación haciendo referencia a los arts. 25 y 26 de la Directiva 95/46 en los que, como ya hemos comentado, se recoge un régimen dirigido a garantizar un control por los Estados miembros de las transferencias de datos personales hacia terceros países. El Tribunal considera que de estos preceptos se extrae la posibilidad de que el control de la garantía de protección de datos personales en el tercer país pueda ser realizado, no sólo por la Comisión, sino también por la autoridad de control de un Estado miembro, aclarando que, si bien es cierto que hasta que una Decisión no sea declarada inválida por el Tribunal de Justicia de la Unión Europea, los Estados miembros y sus órganos no podrán adoptar ningún tipo de medida contraria a la misma. La Decisión 2000/520 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, como es el caso, una solicitud, prevista en el art. 28.4 de la Directiva 95/46, para la protección de sus derechos y libertades frente al tratamiento de esos datos, ni dejar sin efecto ni limitar las facultades expresamente reconocidas a las autoridades nacionales de control por el artículo 8, apartado 3, de la Carta y por el artículo 28 de la referida Directiva" (apartado 53).

De la argumentación expuesta por el Tribunal se desprende que sería contrario a la Directiva 95/46 que una Decisión de la Comisión tuviera el efecto de impedir que una autoridad nacional de control examine la queja de una persona que considera que, con motivo

de operaciones de comercio internacional, se esté vulnerando su derecho a la protección de datos de carácter personal, en los términos reconocidos en la Carta y desarrollados en la Directiva 95/46.

Atendiendo a estas consideraciones, de la Sentencia del TJUE que comentamos se puede extraer, como doctrina general, que cuando un sujeto presenta ante la autoridad nacional de control una solicitud para la protección de sus derechos y libertades frente al tratamiento de esos datos cuando han sido transferidos desde la Unión Europea a un tercer país, e impugna, con ocasión de esa solicitud, como en el asunto principal, una Decisión de la Comisión: "incumbe a esa autoridad examinar la referida solicitud con toda la diligencia exigible" (apartado 63), realizando todas las investigaciones necesarias para esclarecer los hechos y atender a la solicitud del demandante, 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 Tribunal de Justicia de la Unión Europea.

Estamos, por tanto, ante una importante decisión del TJUE de cara a las posibles denuncias que pueden formular los ciudadanos comunitarios ante sus respectivas autoridades de control, pues el TJUE concluye que la Decisión 2000/520 no impide "que una autoridad de control de un Estado miembro, a la que se refiere el artículo 28 de esa Directiva, examine la solicitud de una persona relativa a la protección de sus derechos y libertades frente al tratamiento de los datos personales que la conciernen que se hayan transferido desde un Estado miembro a ese tercer país, cuando esa persona alega que el Derecho y las prácticas en vigor en este no garantizan un nivel de protección adecuado" (apartado 66).

5.4. Sobre la validez de la Decisión de adecuación de la Comisión

Una vez aclarada la extensión de las facultades de las autoridades de control de los Estados miembros, el TJUE pasa a examinar 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, tal y como exige el art. 25.2 de la Directiva 95/46/CE[46]

[46] El art. 25.2 establece: "Sin perjuicio de lo dispuesto en el apartado 1, los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado con arreglo al apartado 2 del artículo 25, cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de

y, en consecuencia, si la Decisión y los *Principios de Puerto Seguro* que figuran su anexo I, se ajustan a las exigencias derivadas de la Directiva 95/46, interpretada a la luz de la Carta.

El Tribunal constata que, en virtud del anexo I de la Decisión 2000/520, 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 pueden acceder a dichos datos, como también 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 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 Estados Unidos, dado el carácter general de la excepción prevista en el anexo I.

En mi opinión, este pronunciamiento del Tribunal de Justicia está muy condicionado por las revelaciones hechas a la prensa por el Sr. Edward Snowden, pues, si bien no hay ninguna referencia a las mismas en la fundamentación del fallo, si la hay a la Comunicación COM (2013) 846 final, que anteriormente comentamos, y que el Tribunal trae a colación, pese a que se dictó con posterioridad a la presentación de la demanda ante el Tribunal de Justicia irlandés, y en la que, como ya hemos analizado en el epígrafe anterior, la Comisión valoró negativamente que las autoridades estadounidenses pudieran acceder a los datos personales transferidos desde la Unión Europea y tratarlos de manera incompatible con las finalidades de la transferencia, sin estar sometidas a ningún parámetro de control respecto de la necesidad y proporcionalidad de dicha injerencia, a lo que se une la confirmación de que "las posibles personas afectadas no disponían de unas vías jurídicas administrativas o judiciales que les permitieran acceder a los datos que les concernían y obtener, en su caso, su rectificación o supresión" (apartado 90).

las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas".

5.5. La doctrina del TJUE en relación con los estándares de protección de los datos de carácter personal

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), siendo imprescindible que las personas cuyos datos personales resulten afectados "dispongan de garantías suficientes que permitan proteger eficazmente sus datos personales contra los riesgos de abuso y contra cualquier acceso o utilización ilícitos de éstos. La necesidad de disponer de esas garantías es aún más importante cuando los datos personales se someten a un tratamiento automático y existe un riesgo elevado de acceso ilícito a ello" (apartado 91).

b) La regulación de cualquier actuación que pueda limitar el derecho fundamental a la intimidad garantizado en la Unión Europea y, de forma más concreta, el derecho fundamental a la protección de datos de carácter personal, deberá ceñirse a lo estrictamente necesario, sin que pueda considerarse válida una normativa que autorice de forma generalizada el acceso a los datos personales "sin el establecimiento de diferenciaciones, limitaciones o excepciones ni la prevención de criterios objetivos que permitan determinar los casos en los que cabe que una autoridad pública pueda acceder y utilizar los datos" (apartado 94).

c) 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).

d) 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).

e) Las autoridades nacionales de control tienen la facultad de examinar cualquier solicitud de protección de los derechos y libertades de una persona residente en dicho Estado, frente a todo tratamiento de datos personales que la afecte, 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, al entender que la Comisión no constató suficientemente la existencia de un nivel de protección adecuado de los datos de carácter personal transferidos a Estados Unidos, unido al hecho de que el art. 3.1 de la Decisión 2000/520 priva a las autoridades nacionales de control de las facultades que les atribuye el artículo 28 de la Directiva 95/46.

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 de la Comisión, todas las entidades estadounidenses antes adheridas al *Acuerdo de Puerto Seguro*[47], 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 la encontramos en el art. 26.1 de la Directiva 95/46, que, tal y como hemos reproducido anteriormente, regulaba la posibilidad de que 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.

Parece que con este catálogo de posibilidades se buscaba no bloquear, ni entorpecer, las relaciones económicas y comerciales entre Europa y terceros países, pero, en mi opinión,

[47] Según el punto 2.2 de la Comunicación COM (2013) 847 final, a 26 de septiembre de 2013 estaban certificadas un total de 3246 entidades.

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 art. 8 de la Carta de Derechos Fundamentales de la Unión Europea, 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 respecto a sus datos personales, pudiendo controlar el acceso y tratamiento de los mismos. Sin embargo, creo que la exigencia derivada del art. 25.1 de la Directiva 95/46, según la cual las transferencias de datos personales a países terceros sólo podrán realizarse cuando dicho país garantice "un nivel de protección adecuado", queda vacía de contenido si cede con el sólo consentimiento del interesado, tal y como se desprendía del art. 26.1 a) de la Directiva 95/46.

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" 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.

Las *cláusulas contractuales tipo* son un instrumento que permite a los responsables de tratamiento realizar transferencias internacionales de datos con ciertas garantías,

subscribiendo un contrato entre el importador y el exportador de los datos. En ellas se deben determinar aquellas medidas de seguridad, técnicas y organizativas, que han de ser aplicadas por los encargados del tratamiento 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[48].

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 un encargado situado en un país que no cuenta con un nivel de protección adecuado.

El medio para la aprobación de unas y otras es diferente. Mientras que las *cláusulas contractuales tipo* deberán ser adoptadas por la Comisión por medio de Decisiones, de acuerdo con lo previsto en el art. 26.4 de la Directiva 95/46, según el cual: "Cuando la Comisión decida, según el procedimiento establecido en el apartado 2 del artículo 31, que determinadas cláusulas contractuales tipo ofrecen las garantías suficientes establecidas en el apartado 2, los Estados miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión", las *normas corporativas vinculantes* deberán ser aprobadas por las autoridades de control de protección de datos de los diferentes países, valorando su adecuación a los principios de la Directiva 95/46.

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 Estados Unidos. No obstante, lo que no resultaba asumible era que dichas relaciones comerciales se vieran afectadas negativamente, por lo que se siguieron realizando transferencias internacionales de datos entre ambos países con la exclusiva garantía de las *cláusulas contractuales tipo* y de las *normas corporativas vinculantes*, aunque su eficacia dependía de que ninguna de las autoridades de control de protección de datos de cualquiera de los países miembros considerase, tras una investigación, la ilicitud de la transferencia y su consiguiente suspensión o prohibición.

[48] 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.

Debido a que esta situación resultaba insostenible, 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 Norteamericana en el acceso a los datos personales que llegaban 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.

En esta Decisión de Ejecución la Comisión indica, en síntesis[49], que se ha producido una mejora en las garantías de protección de los datos personales trasferidos desde la Unión Europea a 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.

[49] Síntesis realizada a partir del Considerando número 65 de la Decisión que estamos analizando.

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 mercantiles podrían verse afectadas seriamente. En este sentido, quisiera llamar la atención respecto del contenido del considerando número 111 y siguientes de la Decisión de Ejecución (UE) 2016/1250, de los que se desprende que el Gobierno estadounidense indicó expresamente a la Comisión una serie de vías jurídicas de protección que se ofrecen a los ciudadanos de la UE para hacer valer su derecho a la protección de datos de carácter personal. Así, sin ánimo exhaustivo:

a) En el considerando número 112 se contempla la posibilidad que tiene toda persona de interponer una demanda de indemnización por daños y perjuicios económicos contra los Estados Unidos cuando se haya utilizado o divulgado información sobre ella de manera intencionada y no autorizada; la facultad de demandar a funcionarios públicos estadounidenses a título personal por los daños y perjuicios económicos ocasionados a partir de esta vulneración; y la posibilidad de impugnar la legalidad del acceso a los datos personales (y solicitar la destrucción de la información y de los datos obtenidos) en el supuesto de que el Gobierno de los Estados Unidos pretenda utilizar o divulgar cualquier información obtenida o derivada de la vigilancia electrónica.

b) El Gobierno estadounidense también indicó a la Comisión una serie de vías adicionales que los interesados de la UE podían utilizar para presentar un recurso contra determinados funcionarios por el acceso no autorizado a datos personales y por la utilización de estos por parte del Gobierno, incluso en el caso de que se hubieran obtenido con presuntos fines de seguridad nacional. Se especifica en el considerando número 113 que esta posibilidad de incoar un procedimiento se refiere a la protección de datos a partir del acceso ilegal (por ejemplo, el acceso remoto a un ordenador a través de Internet) y pueden invocarse en determinadas circunstancias (tales como la comisión de actos intencionados o premeditados, o actos al margen de las propias funciones).

c) *La Administrative Procedure Act* (Ley de procedimiento administrativo) ofrece una posibilidad de recurso más general (título 5, artículo 702) según el cual toda persona que sufra un perjuicio a causa de actuaciones de una agencia o que se haya visto adversamente afectada o perjudicada por la acción de una agencia, tiene derecho a interponer un recurso judicial. Esto incluye la posibilidad de solicitar al

órgano jurisdiccional que declare ilegales y anule la actuación, los resultados y las conclusiones de la agencia que sean resultado de una actividad arbitraria.

A pesar de estos avances, subsistieron algunas objeciones serias que el Parlamento Europeo puso de manifiesto en su Resolución, de 26 de mayo de 2016, sobre los flujos transatlánticos de datos, en la que felicita por las mejoras que introduce la Decisión de Ejecución 2016/1250 de la Comisión, pero en la que también pone de relieve algunas de sus deficiencias, como que el Defensor del Pueblo estadounidense no es una institución suficientemente independiente (es nombrado por el Secretario de Estado); que el acceso a datos por parte de las autoridades públicas sigue sin someterse a un estricto test de necesidad y proporcionalidad; y que la mayoría de los recursos jurisdiccionales que se ofrece a los ciudadanos europeos resultan excesivamente complejos.

Como veremos a continuación, 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.

7. ANÁLISIS DE LA SENTENCIA SCHREMS II (STJUE DE 16 DE JULIO DE 2020, EN EL ASUNTO *DATA PROTECTION COMMISSIONER* vs. *FACEBOOK IRELAND LIMITED y MAXIMILLIAN SCHREMS*)

7.1. Antecedentes y normativa aplicable

Como consecuencia de la Sentencia Schrems I, de 6 de octubre de 2015, mediante la que el Tribunal de Justicia declaró invalida la Decisión 2000/520/UE, la *High Court* de Irlanda anuló la desestimación de la reclamación del Sr. Schrems y se la devolvió al Comisario para que continuara con el procedimiento y realizara las investigaciones pertinentes.

Abierto de nuevo el procedimiento, el Comisario llegó a la conclusión de que sin la cobertura jurídica de una Decisión de adecuación de la Comisión, los 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 *National Security Agency* (NSA) y la *Federal Bureau of Investigation* (FBI), 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 Carta de derechos fundamentales de la UE 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 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 sólo 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 de 6 de octubre de 2015 (caso 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 Tribunal de Justicia de la Unión Europea, 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*, imponiendo obligaciones más estrictas a las empresas estadounidenses en la protección de los datos personales que son transferidos desde la Unión

Europea y exigiendo una intervención más restrictiva y controlada por parte de la Agencia de Seguridad Norteamericana.

Ahora bien, como analizaremos más adelante, en las cuestiones prejudiciales cuarta, quinta, novena y décima, 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 Tribunal de Justicia de la Unión Europea 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 también debe tomarse en consideración esta última Decisión de Ejecución de la Comisión, vigente desde el 12 de julio de 2016[50].

También es importante indicar que el TJUE aclara, en los antecedentes (apartados 69 y siguientes), una serie de aspectos procesales y materiales relevantes para la resolución de las cuestiones prejudiciales que se plantean, que pueden sintetizarse en dos puntos:

a) Por un lado, indica que, si bien en virtud del art. 94.1 RGPD la Directiva 95/46 fue derogada con efecto a partir del 25 de mayo de 2018, la Directiva estaba todavía en vigor en el momento de la formulación, el 4 de mayo de 2018, de la petición de decisión prejudicial. Asimismo, los artículos 3.2, 25, 26 y 28.3 de la Directiva 95/46, a los que se refieren las cuestiones prejudiciales, fueron, en esencia, reproducidos en los artículos 2.2, 45, 46 y 58 del RGPD, respectivamente. Por ello, el hecho de que el órgano jurisdiccional remitente haya formulado las cuestiones prejudiciales refiriéndose únicamente a las disposiciones de la Directiva 95/46, ya derogada, no puede dar lugar a la inadmisibilidad de la presente petición de decisión prejudicial.

b) Por otro lado, y en conexión con el punto anterior, el TJUE entiende que no hay óbices procesales para que las cuestiones prejudiciales planteadas se resuelvan de acuerdo con las disposiciones del nuevo RGPD y no de la Directiva 95/46, ya derogada, pues el Tribunal de Justicia está obligado a pronunciarse aplicando al caso la normativa vigente de la Unión y, además, hay que recordar que el Tribunal de Justicia tiene la misión de interpretar cuantas disposiciones del Derecho de la Unión sean necesarias para que los órganos jurisdiccionales nacionales puedan resolver los litigios que se les haya sometido, aun cuando tales disposiciones

[50] En el apartado 151 de la STJUE que analizamos se exponen las razones por las que el TJUE considera necesario examinar también la validez 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*, aunque no fue impugnada por el Comisario.

no se mencionen expresamente en las cuestiones remitidas por dichos órganos jurisdiccionales[51].

Tras estas aclaraciones preliminares, el TJUE entra a resolver las 11 cuestiones prejudiciales elevadas por la *High Court*, que pueden agruparse en torno a los apartados que exponemos a continuación.

7.2. El TJUE afirma que el RGPD protege frente al tratamiento de datos personales de ciudadanos comunitarios realizado por las autoridades de un país tercero

En la primera cuestión prejudicial el órgano jurisdiccional irlandés solicitó, en esencia, que se esclareciera si estaba comprendida dentro del ámbito de aplicación de la Directiva 95/46/CE una transferencia de datos personales realizada por un operador económico establecido en un Estado miembro a otro operador económico establecido en un país tercero, cuando, en el transcurso de esa transferencia o con posterioridad, esos datos pudieran ser tratados por las autoridades de ese país tercero con fines de seguridad nacional, defensa y seguridad del Estado[52].

El TJUE, tras recordar que todas las pregunta se responderán a la luz de lo dispuesto en el RGPD, que deroga la Directiva 95/46/CE, responde afirmativamente, razonando que el RGPD obliga explícitamente a la Comisión, cuando evalúa la adecuación del nivel de protección ofrecido por un país tercero, a tener en cuenta todo el ordenamiento jurídico de dicho país, incluida la relativa a la seguridad pública, la defensa y la seguridad nacional, así como las posibilidades de acceso de las autoridades públicas a los datos personales que se encuentran en bases de datos de empresas y entidades comerciales (apartado 87), añadiendo que el propio tenor del art. 45.2.a) RGPD[53], pone de manifiesto el hecho de que el eventual

[51] El TJUE cita en este sentido su STJUE de 2 de abril de 2020, Ruska Federacija (C-897/19 PPU, EU:C:2020:262), apartado 43 y jurisprudencia citada.

[52] Cuestión que habrá de resolverse interpretando el artículo 2, apartados 1 y 2, letras a), b) y d), del RGPD, en relación con el artículo 4 TUE, apartado 2.

[53] El art. 45.1 RGPD dispone que: "Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica". En el apartado segundo se recogen una serie de parámetros que tendrá que aplicar la Comisión para evaluar "la adecuación del nivel de protección". Finalmente en el tercer apartado de este artículo se recoge que, tras dicha evaluación de adecuación, la Comisión "podrá decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno

tratamiento por un país tercero de los datos en cuestión con fines de seguridad pública, defensa y seguridad del Estado, no pone en entredicho la aplicabilidad del RGPD.

Como se puede deducir fácilmente, esta cuestión de fondo ya había sido resuelta en la STJUE Schrems I, sin perjuicio de que ahora los razonamientos se derivan de la aplicación del RGPD y no de la Directiva.

7.3. Garantías que han de rodear a las *cláusulas contractuales tipo* de protección de datos

Las cuestiones prejudiciales segunda, tercera y sexta nos remiten a una única pregunta, que gira en torno a la necesidad de que el TJUE concrete cuáles han de ser las garantías que han de cumplirse para una efectiva protección de los datos de carácter personal de acuerdo con lo previsto en el RGPD, en aquellos casos en que se realizan transferencias de datos a un tercer país respecto del que no existe una "decisión de adecuación" adoptada por la Comisión en los términos previstos en el art. 45 RGPD y, por tanto, en aquellos casos en que han de utilizarse las *cláusulas contractuales tipo* a las que se refiere el art. 46 RGPD[54].

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

o varios sectores específicos de un tercer país, o una organización internacional garantizan un nivel de protección adecuado (…)", fijando a tal efecto mecanismo de revisión periódica, al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional.

[54] El art. 46.1 RGPD recoge que: "A falta de decisión con arreglo al artículo 45, apartado 3, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas". Las garantías adecuadas a las que se refiere este apartado podrán ser aportadas sin que se requiera ninguna autorización expresa de ninguna autoridad de control en una serie de supuestos que se especifican en el art. 46.2 RGPD, de entre los que se encuentran la existencia de *cláusulas tipo de protección de datos*.

que los interesados cuenten con "derechos efectivos y exigibles" y con "recursos administrativos y acciones judiciales que sean efectivos".

Asimismo, para entender el nivel de protección exigido por el Reglamento, debemos acudir al artículo 44 RGPD que contempla lo que podríamos calificar como un principio general que han de cumplir todas las trasferencias de datos personales a terceros países, 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.

Pues bien, para dar respuesta a esta cuestión, el TJUE considera que hay que interpretar lo dispuesto en el art. 46, apartados 1 y 2 del RGPD, relativo a las transferencias de datos personales a un país tercero basadas en *cláusulas contractuales tipo* de protección de datos, entendiendo que también en estos supuestos es imprescindible constatar que los datos transferidos "gozan de un nivel de protección sustancialmente equivalente al garantizado dentro de la Unión" (apartado 105), aclarando que, en la evaluación del nivel de protección garantizado en el contexto de una transferencia de esas características, la Comisión debe tomar en consideración "tanto las estipulaciones contractuales acordadas entre el responsable o el encargado del tratamiento establecidos en la Unión y el destinatario de la transferencia establecido en el país tercero de que se trate como, por lo que atañe a un eventual acceso de las autoridades públicas de ese país tercero a los datos personales de ese modo transferidos, los elementos pertinentes del sistema jurídico de dicho país y, en particular, los mencionados en el art. 45.2, del referido Reglamento" (apartado 105).

7.4. Competencias de las autoridades de control de los Estados miembros de la Unión Europea

En la octava cuestión prejudicial, la *High Court* pregunta si, con apoyo en la normativa de la Unión, 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.

La respuesta del TJUE es afirmativa, lo que supone otorgar a las autoridades de control de cada uno de los Estados miembros un papel muy relevante en la protección de los datos de carácter personal que se transfieren a terceros países, hasta el punto de que pueden cuestionar la valoración realizada por la Comisión respecto de las garantías ofrecidas por las *cláusulas contractuales tipo.*

Así, el TJUE fija una doctrina muy clara en relación con el importante papel que tienen en la Unión Europea las autoridades de control de cada uno de los Estados miembros, sosteniendo (apartado 107) que 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 y, por tanto, cada una de ellas está investida de competencia para comprobar si una transferencia de datos personales desde el Estado miembro de esa autoridad, hacia un tercer país, respeta las exigencias del RGPD, jurisprudencia que ya se había adelantado en la STJUE de 6 de octubre de 2015 (Schrems I), como hemos analizado anteriormente[55].

Partiendo de esta competencia general, el TJUE recuerda que las autoridades de control tienen como función primordial asegurar la correcta aplicación del RGPD y velar por su cumplimiento, lo que pasa a tener una especial importancia en el contexto de las transferencia de datos personales a un país tercero, dado que, como se desprende del propio tenor del considerando 116 del RGPD "cuando los datos personales circulan a través de las fronteras hacia el exterior de la Unión se puede poner en mayor riesgo la capacidad de las personas físicas para ejercer los derechos de protección de datos, en particular con el fin de protegerse contra la utilización o comunicación ilícitas de dicha información". En ese supuesto, tal como se precisa en ese mismo considerando, "es posible que las autoridades de control se vean en la imposibilidad de tramitar reclamaciones o realizar investigaciones relativas a actividades desarrolladas fuera de sus fronteras".

Pues bien, para facilitar el cumplimiento de su misión y la posibilidad de tramitar las reclamaciones presentadas, el art. 58.1 RGPD atribuye a las autoridades de control

[55] Véase el apartado 47 de la sentencia de 6 de octubre de 2015, Schrems, C-362/14, EU:C:2015:650.

importantes poderes de investigación[56], por lo que el TJUE indica, en la Sentencia que analizamos, 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 de modo adecuado con el fin de subsanar la insuficiencia constatada.

En todo caso, lo que ahora interesa destacar y que constituye el núcleo de la octava cuestión prejudicial, es que el poder de ejecución que el artículo 46.2.c) RGPD reconoce a la Comisión para que adopte y valide *cláusulas contractuales tipo* de protección de datos, no le confiere la competencia para restringir las facultades que el Reglamento otorga a las autoridades de control de cada Estado miembro, que, con total independencia, podrán examinar si la transferencia de estos datos a un país tercero cumple con todas las exigencias contempladas en el RGPD.

En conclusión, el TJUE declara que "la autoridad de control competente está obligada a suspender o prohibir una transferencia de datos a un país tercero basada en cláusulas tipo de protección de datos adoptadas por la Comisión" cuando esa autoridad de control considera que dichas cláusulas no se respetan o no pueden respetarse en ese país tercero y que la protección de los datos transferidos exigida por el Derecho de la Unión no puede garantizarse (apartado 121).

7.5. El TJUE considera válida la Decisión de la Comisión, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a terceros países

El TJUE considera necesario examinar conjuntamente las cuestiones prejudiciales séptima y undécima, pues en ambas se pone en duda la validez de la Decisión de la Comisión, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de

[56] El art. 58.1 RGPD fija que "Cada autoridad de control dispondrá de todos los poderes de investigación indicados a continuación: a) ordenar al responsable y al encargado del tratamiento y, en su caso, al representante del responsable o del encargado, que faciliten cualquier información que requiera para el desempeño de sus funciones; b) llevar a cabo investigaciones en forma de auditorías de protección de datos; c) llevar a cabo una revisión de las certificaciones expedidas en virtud del artículo 42, apartado 7; d) notificar al responsable o al encargado del tratamiento las presuntas infracciones del presente Reglamento; e) obtener del responsable y del encargado del tratamiento el acceso a todos los datos personales y a toda la información necesaria para el ejercicio de sus funciones; f) obtener el acceso a todos los locales del responsable y del encargado del tratamiento, incluidos cualesquiera equipos y medios de tratamiento de datos, de conformidad con el Derecho procesal de la Unión o de los Estados miembros".

datos personales a los encargados del tratamiento establecidos en terceros países, a la luz de los artículos 7, 8 y 47 de la Carta. En concreto, el Tribunal Europeo se ve en la necesidad de examinar si esta Decisión garantiza la seguridad de los datos personales transferidos a un tercer país, en la medida en la que las *cláusulas contractuales tipo* no son vinculantes para las autoridades de esos países terceros (sólo lo son para la entidad comercial destinataria primera de los mismos). Este problema se produce, como se puede deducir fácilmente, cuando el ordenamiento jurídico de ese país tercero permite a sus autoridades públicas llevar a cabo injerencias en bases de datos de carácter personal, invocando genéricos motivos de interés nacional.

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).

7.6. Se declara la nulidad de 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

El TJUE agrupa para su examen las cuestiones prejudiciales cuarta, quinta, novena y décima, pero, con carácter preliminar, 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 adoptar 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.

En consecuencia, para dar respuesta a estas cuestiones el TJUE no sólo examina si las transferencias de datos a los Estados Unidos con la cobertura de las *cláusulas contractuales tipo* previstas en la Decisión, de 5 de febrero de 2010, vulneran los derechos de los artículos 7, 8 y 47 de la Carta (duda que nace a partir de las investigaciones realizadas por la propia *High Court* en relación con la normativa de los Estados Unidos), sino que también va a estudiar si 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.*

El TJUE aborda el estudio de las cuestiones planteadas tomando como marco lo dispuesto en los arts. 7 y 8 de la Carta, que forman parte del nivel de protección exigido dentro de la Unión y cuyo respeto debe ser constatado por la Comisión antes de adoptar una Decisión de adecuación en virtud del artículo 45.1 RGPD, pero recordando también que, si bien los derechos a la intimidad y a la protección de datos de carácter personal no tienen un carácter absoluto (apartado 172), todo límite tiene que estar previsto en una ley, tiene que ser proporcional y no podrá afectar a su contenido esencial (apartados 174 y ss.).

En el caso que nos ocupa 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 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 reciente 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 UE 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 establecían 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 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[57], lo que ya es una realidad respecto de las actividades que se materializan a través de servicios de *cloud computing*[58].

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 art. 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:

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;

c) la transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica;

---

[57]Véase, por lo que tuvo de pionero: TAPSCOTT, D.: *The digital economy: promise and peril in the age of networked intelligence*, New York: McGraw-Hill, 1997. El término "economía digital" se generalizó tras la publicación del citado libro de Tapscott, en el que se auguraba, en la década de os noventa, cómo Internet iba a cambiar la forma de hacer negocios. De hecho, se trata de uno de los libros más vendidos en 1997, apareciendo en diversas listas de *best-sellers*, como la lista de libros de negocios del *New York Times* y la lista de *BusinessWeek*.

58 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 interesante estudio de los comienzos del *cloud computing* en: TORRES VIÑALS, J.: *Del cloud computing al big data,* UOC (Universitat Operta de Catalunya), 2012. También resulta de interés, por su enfoque jurídico: MARTÍNEZ MARTÍNEZ, R.: *Derecho y cloud computing*, Civitas, Pamplona, 2012.

d) la transferencia sea necesaria por razones importantes de interés público;

e) la transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones;

f) la transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento;

g) 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 sólo 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 art. 26 de la Directiva 95/46, en el que, como ya hemos comentado, el consentimiento del interesado en la cesión y en el tratamiento de sus datos de carácter personal se convierte en la vía fácil para superar todas las exigencias derivadas de las normas jurídicas de la Unión Europea en materia de protección de datos personales, pues si el interesado desea obtener determinados servicios de una empresa norteamericana, 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 In.* 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[59].

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

[59] MIGUEL ASENSIO, P. A. (de): "Implicaciones de la declaración de invalidez del Escudo de Privacidad". *La Ley Unión Europea*, núm. 84, septiembre 2020, p. 7.

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.

Así, 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[60].

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[61].

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.

En consecuencia, la transferencia de datos de carácter persona entre la Unión Europea y EE. UU. 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 sólo acudiendo a los supuesto previstos en el art. 49 RGPD, anteriormente reproducido, sino también mediante la utilización de alguno de los mecanismos subsidiarios de protección regulados en los artículos 45 y ss. del RGPD, que

[60] 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.

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

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[62], 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,* tienen 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 las 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, pus 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[63], pues no se espera que los Estados Unidos modifiquen sus políticas de vigilancia[64], dada la permanencia de instrumentos de vigilancia como los recogidos en la FISA o en la E.O. 12333, en concreto los programas PRISM y Upstream[65].

Por tanto, anulados sendos Acuerdos, la facultad de determinar y evaluar las garantías necesarias para reanudar las transferencias de datos a EE. UU. se traslada a las autoridades

---

[62] Un interesante análisis de los códigos privados de conducta de las empresas que operan en redes sociales en: GARCÍA-PERROTE MARTÍNEZ, I., y GABRIEL GARCÍA-MICÓ, T.: "Identidad, cesión de datos personales y la decisión Privacy Shield tras la STJUE Schrems II", *Indret: Revista para el Análisis del Derecho,* núm. 3, 2020, pp. 555 y ss.

[63] COSTELLO, R. A.: "Schrems II: Everything is Illuminated?", *European Papers*, 2020, p. 16.

[64] Sobre el acceso a los datos de carácter personal por pate de las autoridades norteamericanas: CHANDER, A.: "Is Data Localization a Solution for Schrems II?", *Journal of International Economic Law*, núm. 23, 2020, p. 775.

[65] BUTLER, A.: "United States. Whither privacy shield in the Trump Era". *European Data Protection Law Review*, núm. 3, 2017, p. 112.

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[66].

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 sólo 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 UE[67] 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"[68]. Para De Miguel, esta Sentencia "pone una vez más de relieve la deficiente aplicación de la legislación de la Unión Europea en la materia"[69].

9. LAS RECOMENDACIONES 01/2020 DEL COMITÉ EUROPEO DE PROTECCIÓN DE DATOS

Tras las declaraciones de nulidad de las Decisiones de adecuación de la Comisión respecto de los Estados Unidos, como consecuencia de las SSTJUE Schrems I y Schrems II, no sólo 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, como se ha intentado explicar en las páginas

[66] Lo que pone de relieve FUENTES MÁIQUEZ, A.: "Comentario de la STJUE de 16 de Julio de 2020, C-311/18 (Schrems II)", *Revista de la Facultad de Derecho (ICADE)*, enero, 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, S. C.: "Eu privacy shield: Practical implications for U.S. litigation". *Practical Lawyer*, núm. 62, 2016, pp. 60 a 64.

[67] TRACOL, X.: "Schrems II: The return of the Privacy Shield". *Computer Law & Security Review,* núm. 39, 2020, p. 5; MALDONADO, E.: "Bridging the gap in transatlantic data protection", *Discussion Paper*, No. 4/20. Europa-Kolleg Hamburg, Institute for European Integration, p. 10; MIGUEL ASENSIO: "Implicaciones de la declaración de invalidez del Escudo de Privacidad", op.cit., p. 6.

[68] FUENTES MÁIQUEZ, A.: "Comentario de la STJUE de 16 de Julio de 2020, C-311/18 (Schrems II)", *op. cit.,* p. 8.

[69] En: "Implicaciones de la declaración de invalidez del Escudo de Privacidad", *op. cit*., p. 7.

precedentes, 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 Estados Unidos; ya sea por el eventual uso desleal de estos datos por empresas que, pese a suscribir *claúslulas corporativas vinculante*, incumplen dichos acuerdos y su domicilio social se encuentra en un país que no ofrece garantías jurisdiccionales suficientes para los afectados), 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 determinados Estados o preservar sus datos personales frente a un uso indebido de los mismos.

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 UE, 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.

Con la finalidad de ayudar a los exportadores de datos europeos a realizar la difícil tarea de evaluar el nivel de protección de los datos personales en terceros países, el Comité Europeo de protección de datos adopta estas Recomendaciones, sistematizando una serie de pasos a seguir, indicando algunas fuentes de información que pueden resultar útiles y mostrando algunos ejemplos de medidas complementarias que pueden ser aplicadas.

Con la primera recomendación se pretende que los exportadores de datos personales conozcan con detalles sus transferencias de datos personales, clasificándolas de manera que tengan certeza de todos los datos que se transfieren y del lugar al que van dirigidos, para así

poder garantizar que el país en cuestión otorga un nivel de protección de los datos trasferidos, esencialmente equivalente a aquel asegurado dentro de la Unión. Esta clasificación deberá tener en cuenta igualmente los fines para los que son transferidos los datos y los ulteriores tratamientos que puedan ser realizados por la entidad receptora.

La segunda recomendación está dirigida a identificar cuál de los mecanismos de garantía previstos en el capítulo V del RGPD está amparando la transferencia. Por supuesto, en aquellos casos en los que exista una Decisión de adecuación de la Comisión no será necesaria ningún tipo de medida adicional. En caso contrario, se deberá recurrir a alguno de los instrumentos de transferencia recogidos en el artículo 46 RGPD si se trata de transferencias periódicas, o a las excepciones del artículo 49 RGPD, en aquellos casos en los que se traten de transferencias ocasionales.

La tercera recomendación consiste en la necesidad de evaluar la legislación y la práctica desarrollada en el tercer país, en todas aquellas cuestiones que puedan afectar a los datos personales transferidos. Así, deberá estudiarse, entre otras cuestiones, la legislación del tercer país sobre el acceso a los datos por parte de las autoridades públicas por razones de "seguridad nacional". Como indica el Comité Europeo de Protección de Datos, esta evaluación deberá ser exhaustiva, diligente y documentada, dado que la entidad responsable de la transferencia de datos tendrá que rendir cuentas de la decisión tomada.

La cuarta recomendación se refiere a la determinación y adopción de aquellas medidas complementarias consideradas necesarias para adaptar el nivel de protección del país en cuestión a las exigencias de la normativa comunitaria, evidentemente, estas medidas complementarias deberán ser ideadas para el caso concreto, dado que dependiendo del país y del instrumento del RGPD en el que esté basada la transferencia de datos, la efectividad de las mismas puede cambiar. En aquellos casos en los que se considere que ninguna medida complementaria es capaz de garantizar, en el país de destino, un nivel de protección esencialmente equivalente al que brinda la Unión Europea, el Comité Europeo de Protección de Datos recomienda suspender las transferencias de datos pues no queda asegurada su protección[70].

La quinta recomendación, en directa conexión con la cuarta, se refiere a la necesidad de adoptar cualquier procedimiento formal necesario para la ejecución de las medidas

[70] En el anexo 2 del documento recoge una serie de ejemplos de medidas complementarias que pueden ser adoptadas por la entidad responsable de la transferencia de datos personales, como el cifrado previo de los datos personales.

complementarias acordadas. Con la finalidad de agilizar estos procedimientos, se indica que no es necesario que la autoridad de control competente examine y autorice este tipo de cláusulas o garantías adicionales, siempre que las medidas complementarias identificadas no contravengan, directa ni indirectamente el RGPD. Es decir, el exportador y el importador de datos deberán garantizar que las cláusulas adicionales no puedan interpretarse en el sentido de que restringen los derechos y obligaciones que se derivan de la normativa comunitaria.

La sexta y última recomendación se refiere a la necesidad de hacer un seguimiento continuo de la evolución de la normativa del tercer país al que se hayan transferido datos personales, de cuyo resultado dependerá que se sigan manteniendo las decisiones tomadas de acuerdo con las cinco recomendaciones anteriormente expuestas.

10. LA TRANSFERENCIA INTERNACIONAL DE DATOS EN EL ACTUAL REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS

10.1. Requisitos generales de las Transferencias internacionales de datos de acuerdo con el RGPD

Como se ha adelantado, el RGPD dedica un capítulo específico (el Capítulo V) a las transferencias de datos personales a terceros países u organizaciones internacionales, dedicando a tal finalidad los artículos 44 a 50. Asimismo, del análisis de la STJUE Schrems II, se desprende que el TJUE lleva a cabo una interpretación muy rigurosa de los preceptos del RGPD relativos a las transferencias internacionales de datos, con la finalidad de que las previsiones de este texto jurídico tengan una aplicación práctica efectiva.

Todos los preceptos del Capítulo V están dirigidos a asegurar que el nivel de protección de las personas físicas garantizado en el RGPD no se vea dañado como consecuencia de las transferencias de datos personales a terceros países, por ello en el art. 44 RGPD se dispone, con carácter general, como ya hemos visto, que sólo se realizarán transferencias de datos personales que sean objeto de tratamiento o que vayan a serlo tras su transferencia a un tercer país u organización internacional si "a reserva de las demás disposiciones del presente Reglamento, el responsable y el encargado del tratamiento

cumplen las condiciones establecidas en el presente capítulo, incluidas las relativas a las transferencias ulteriores de datos personales desde el tercer país u organización internacional a otro tercer país u otra organización internacional".

Con la finalidad de cumplir este objetivo, y en unos términos similares a como lo hacía la Directiva 95/46, el Reglamento fija los distintos supuestos en los que se puede sostener que existen garantías suficientes para que pueda realizarse una transferencia de datos personales a un tercer país u organización internacional.

10.2. Transferencias basadas en una Decisión de adecuación

El art. 45.1 RGPD dispone que sólo podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, o la organización internacional de que se trate "garanticen un nivel de protección adecuado", que es lo que se viene denominando como "transferencias basadas en una Decisión de adecuación". Asimismo, el Reglamento fija unos parámetros que la Comisión ha de tener en cuenta para evaluar la adecuación del nivel de protección (art. 45.2 RGPD), que, según interpreta el TJUE en la Sentencia Schrems II, resultan bastante exigentes, sobre todo en lo que se refiere a la existencia de acciones judiciales que sean reales y efectivas. El TJUE también es muy explícito con respecto a la necesidad de que el tercer Estado cuente con una o varias autoridades de control independientes, que tendrán la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos.

Hay que tener en cuenta que antes de que la Comisión estudie el cumplimiento de los requisitos citados en el RGPD, el país en cuestión deberá someterse a un examen previo en el que se valorarán los aspectos que se indican en: "La Comunicación al Parlamento Europeo y al Consejo sobre Intercambio y protección de los datos personales en un mundo globalizado" y que pueden sintetizarse en los siguientes puntos:

a) Se llevará a cabo un previo análisis del alcance de las relaciones comerciales de la UE con el país en cuestión.

b) Se realizará un informe de la magnitud de los flujos de datos personales con origen de la UE que llegan al tercer país.

c) Se valorará si, debido a su avance en la protección de datos y privacidad, el país puede servir de modelo para otros terceros Estados.

d) Por último, se tendrán en cuenta las relaciones políticas e internacionales del país analizado.

Con estas exigencias se busca priorizar las decisiones de adecuación de aquellos países con una relación más intensa con la UE y, por lo tanto, con una mayor necesidad de simplificación de las exigencias vinculadas a las transferencias de datos personales.

Conectado con este artículo encontramos el considerando 103 RGPD que explica cómo, en aquellos casos en los que la Comisión haya dictado una Decisión de adecuación, podrán realizarse transferencias de datos al tercer país en cuestión sin necesidad de una autorización específica, siendo suficiente la presunción de garantía de protección concedida por la Decisión.

La comisión ha dictado Decisiones constatando un nivel de protección adecuado de los datos de carácter personal en Suiza, Canadá, Argentina, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay, Nueva Zelanda, Estados Unidos y Japón. Dado que el RGPD entró en vigor en 2018, la mayor parte de las Decisiones (todas menos la de Japón) fueron tomadas con apoyo en la Directiva 95/46/CE (ya derogada), pero esta circunstancia no afecta a su validez, permaneciendo en vigor hasta que sean modificadas, sustituidas o derogadas por una nueva Decisión de la Comisión.

Por último, la Comisión, tras haber evaluado la adecuación del nivel de protección, podrá decidir, mediante un acto de ejecución, que un tercer país, un territorio o uno o varios sectores específicos de un tercer país, o una organización internacional, garantizan un nivel de protección adecuado. El acto de ejecución establecerá un mecanismo de revisión periódica, al menos cada cuatro años, que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional. Como se desprende del art. 45.3 RGPD, el acto de ejecución especificará su ámbito de aplicación territorial y sectorial, y, en su caso, determinará la autoridad o autoridades de control. Una vez evaluados todos estos elementos por la Comisión, se podrá concluir que un país, un territorio o una organización internacional, garantizan un nivel de protección adecuado.

Cuando la Comisión, al realizar la revisión periódica, compruebe que no se garantiza el nivel de protección adecuado anteriormente constatado, deberá dictar un acto de ejecución destinado a derogar, modificar o suspender la Decisión de adecuación tomada en su día. En cualquier caso, a pesar de estas revisiones periódicas previstas en el RGPD, se exige igualmente que la Comisión lleve a cabo una supervisión permanente de la aplicación práctica de las Decisiones.

Otra de las características de las Decisiones de adecuación es que gozan de un amplio margen de flexibilidad, pues puede constatarse tanto una adecuación "total", como "parcial", del territorio. Por ejemplo, la Decisión de adecuación de Canadá es parcial, debido a que únicamente podrán ser transferidos los datos personales a aquellas empresas enmarcadas en la *Personal Information Protection and Electronic Documents Act*, de tal forma que para que pueda entenderse que una empresa canadiense garantiza un nivel de protección adecuado, es decir, similar a aquel ofrecido dentro de la Unión, deberá aceptar las obligaciones, principios y limitaciones recogidos en dicho Documento.

El principal efecto de una Decisión de adecuación es que no resulta necesaria una autorización específica para la transmisión de datos personales al país u organización internacional en cuestión, siendo equivalente la transmisión en estos casos a aquella realizada entre países miembros de la Unión.

10.3. Transferencias de datos mediante "garantías adecuadas"

En el supuesto de que no exista una Decisión de adecuación con arreglo al artículo 45 RGPD, el responsable o el encargado del tratamiento sólo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido "garantías adecuadas" (tal y como indica el art. 46.1 RGPD) y siempre que los interesados cuenten con derechos exigibles y acciones legales efectivas en el país receptor de los datos. Dichas garantías podrán ser aportadas sin que se requiera ninguna autorización expresa de una autoridad de control, por alguno de los siguientes medios (art. 46.2 RGPD):

a) por un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos.

b) por *normas corporativas vinculantes* de conformidad con el artículo 47 RGPD.

c) por *cláusulas tipo* de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 93, apartado 2 RGPD.

d) por *cláusulas tipo* de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión con arreglo al procedimiento de examen a que se refiere en el artículo 93, apartado 2 RGPD.

e) por un código de conducta aprobado con arreglo al artículo 40 RGPD, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados.

f) por un mecanismo de certificación aprobado con arreglo al artículo 42 RGPD, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados.

En este precepto se prevé, con remisión al art. 47 RGPD, que la autoridad de control competente podrá aprobar *normas corporativas vinculantes*, con el fin de contribuir a la aplicación coherente del Reglamento. Las *normas corporativas vinculantes* o *Binding Corporate Rules* (BCR), forman parte de las políticas de protección de datos que se aprueban dentro de un grupo o unión de empresas establecidas en la Unión Europea para gestionar las transferencias datos personales fuera del territorio comunitario. Su objetivo es el de ofrecer garantías suficientes en aquellos casos en los que se van a producir transferencias de datos personales a uno o varios responsables o encargados situados en un tercer país respecto al cual no existe una Decisión de adecuación de la Comisión que certifique la existencia de un nivel de protección adecuado. Se trata por lo tanto de una solución contractual que vincula jurídicamente a las partes de una transferencia internacional de datos, con la finalidad de asegurar en estos casos un nivel de protección acorde con las exigencias establecidas en la Unión Europea.

Las "garantías adecuadas" también pueden obtenerse a través de *cláusulas tipo de protección* adoptadas por la Comisión o por una autoridad de control, examinadas en la STJUE Schrems II, que deben asegurar una protección similar a aquella que se ofrece dentro de la Unión y, por tanto, que han de garantizar la capacidad de los interesados de disponer, en el país receptor de los datos, de derechos jurídicamente exigibles y de acciones legales efectivas.

10.4. Excepciones para situaciones específicas

En el caso de que no se cuente con una Decisión de adecuación (art. 45.3 RGPD), ni con las "garantías adecuadas", de conformidad con el artículo 46 RGPD, una transferencia o un conjunto de transferencias de datos personales a un tercer país u organización

internacional únicamente podrá efectuarse si cumple alguna de las condiciones previstas en el art. 49 RGPD, anteriormente reproducidas.

De todas estas excepciones se desprende que pese a todas las exigencias previstas en el Reglamento, relativas a la necesidad de que las transferencias internacionales de datos se realicen solamente cuando exista una decisión de adecuación de la Comisión (art. 45 RGPD), lo cierto es que tal exigencia está rodeada de excepciones y, en última instancia, el consentimiento del afectado resulta suficiente para eximir de responsabilidad a los receptores de los datos, ya sean entes privados o públicos, prescindiendo del hecho de que, en la mayoría de los casos, el interesado no se encuentra en una situación de igualdad con respecto a las empresas receptoras de datos y, menos aún, con respecto a las autoridades públicas de los terceros países.

10.5. Otros preceptos del RGPD que afectan a las Transferencias internacionales de datos

Fuera de Capítulo V, encontramos en el RGPD otros artículos que afectan en cierta medida a las transferencias internacionales de datos, como son:

- El art. 13 RGPD, que obliga a los responsables de los tratamientos de datos a informar a los interesados en aquellos casos en que se tenga la intención de transferir sus datos personales a un tercer país u organización internacional.

- El art.15 RGPD, que suministra al interesado el derecho a ser informado de las garantías adecuadas previstas en el art. 46 RGPD.

- El art. 30 RGPD, que obliga a los responsables del tratamiento a llevar a cabo un registro de las diferentes actividades de tratamiento realizadas, estando entre estas actividades la transferencia de datos personales a un tercer país u organización internacional.

- El art. 40 RGPD, referido a los códigos de conducta que pueden elaborar las asociaciones de responsables de tratamiento con el fin de especificar la aplicación del reglamento.

11. CONCLUSIONES

PRIMERA: 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. En este trabajo se llega a la conclusión de que, través de estas normas la Unión Europea no se han 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 sólo 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.

SEGUNDA. Una vez analizadas las principales normas comunitarias en materia de protección de datos, llegamos a las siguientes conclusiones: (i) la normativa de la Unión Europea ha mantenido una regla general según la cual los Estados miembros deberán asegurar que la transferencia a un país tercero de datos personales que sean objeto de tratamiento (o destinados a ser objeto de tratamiento con posterioridad a su transferencia), únicamente podrá efectuarse cuando el país tercero "garantice un nivel de protección adecuado" lo que se constata cuando la Comisión Europea emite una *Decisión de adecuación*; (ii) en el caso de que no se haya emitido una *Decisión de adecuación*, los Estados miembros podrán autorizar transferencias de datos personales a un tercer país cuando el responsable del tratamiento ofrezca garantías suficientes dirigidas a proteger los datos de naturaleza personal que llegan a sus archivos, lo que se concreta en la existencia de *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 las *normas corporativas vinculantes* (cuando la transferencia de datos se realice entre entidades de un mismo grupo empresarial); (iii) en el caso de que no se de ninguno de los supuestos 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 o, de forma alternativa, si resulta imprescindible para celebrar o ejecutar un contrato en interés del interesado o resulta necesaria para la salvaguarda del interés vital del interesado, entre otras causas.

TERCERA: Las *Decisiones de adecuación de la Comisión*, dirigidas a certificar que un país tercero garantiza un nivel de protección adecuado de los datos personales de los ciudadanos comunitarios que llegan a su territorio, no han resultado eficaces y han puesto en duda la fiabilidad de la Comisión, pues tras las SSTJUE Schrems I y Schrems II, que anulan sendas Decisiones de adecuación de la Comisión, según las cuales Estados Unidos resultaba un país seguro [Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, conocida coloquialmente como *Acuerdo de Puerto seguro* (*Safe Harbour*) y la Decisión de Adecuación, de 12 de julio de 2016, conocida coloquialmente como *Acuerdo de Escudo de la Privacidad* (*privacy shield)*], 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.

CUARTA: El papel del Tribunal de Justicia de la Unión Europea ha resultado esencial, como garante último de los derechos fundamentales reconocidos en la Carta de los Derechos Fundamentales de la Unión Europea, 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. La doctrina que se desprende de la STJUE Schrems I y que se reitera en la STJUE Schrems II, puede sintetizarse en los siguientes puntos:

a) Toda normativa que limite los derechos fundamentales garantizados por los artículos 7 y 8 de la Carta (intimidad y protección de datos personales) debe contener "reglas claras y precisas que regulen el alcance y la aplicación" de la injerencia, siendo imprescindible que las personas cuyos datos personales resulten afectados "dispongan de garantías suficientes que permitan proteger eficazmente sus datos personales contra los riesgos de abuso y contra cualquier acceso o utilización ilícitos de éstos", estos límites han de ser necesarios y proporcionales.

b) Se produce una lesión del derecho fundamental a la tutela judicial efectiva, reconocido en el artículo 47 de la Carta, si el tercer país receptor de datos personales de ciudadanos comunitarios no prevé mecanismos administrativos y judiciales para que el interesado pueda exigir el acceso sus datos personales, su rectificación, su supresión o una indemnización por el uso y tratamiento indebido de los mismos.

c) Se requiere una constatación debidamente motivada por parte de la Comisión europea 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". Ello incluye la constatación de que las autoridades gubernativas del tercer país sólo pueden acceder a los datos personales que contienen empresas privadas, cumpliendo estrictamente los principios de legalidad, necesidad y proporcionalidad, pudiendo recurrirse esta intervención ante un tribunal independiente.

d) Las autoridades nacionales de control de los Estados de la Unión Europea tienen la facultad de examinar cualquier solicitud de protección de los derechos y libertades de una persona residente en dicho Estado, frente a todo tratamiento de datos personales que la afecte, aunque ello implique poner en cuestión la validez de una Decisión de la Comisión que, no obstante, sólo podrá ser anulada por el TJUE.

QUINTA: Ante la ausencia de una Decisión de adecuación de la Comisión serán las *cláusulas contractuales tipo* y las *normas corporativas vinculantes* los únicos mecanismos jurídicos que ofrece la normativa comunitaria para poder realizar transferencias de datos a un país tercero, pues, en ambos casos, las empresas y entidades receptoras de los datos personales de ciudadanos comunitarios deben de cumplir unas rigurosas garantías de protección. Pero lo cierto es que, en el caso de Estados Unidos, no parece que resulten medios jurídicos idóneos, pues sólo vinculan a las partes contratantes, pero no impiden que las autoridades norteamericanas "por

motivos de seguridad nacional", accedan a estos datos, por lo que las garantías exigidas por el TJUE no se cumplen.

SEXTA: De acuerdo con todo lo expuesto, se llega a la conclusión de que 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 de un uso incorrecto de los mismos, ya sea por particulares o por autoridades públicas. Dicho de otro modo, el interesado tiene que optar entre mantener relaciones comerciales con determinados Estados "no seguros" o preservar sus datos personales frente a un uso indebido de los mismos. Así, el derecho fundamental a la protección de datos de carácter personal que, como se desprende de su enunciado, tiene una naturaleza prestacional (pues su reconocimiento implica que los Estados han de articular mecanismos de garantía efectivos para evitar el acceso y tratamiento indebidos por terceros), pasa a ser un derecho de libertad, toda vez que las autoridades públicas se mantienen al margen y es el individuo el que elige entre renunciar al ejercicio de este derecho o preservar sus datos personales y no realizar determinadas operaciones comerciales.

12. REFERENCIAS BIBLIOGRÁFICAS Y OTROS RECURSOS

A) LIBROS Y ARTÍCULOS

- AGUADO RENEDO, C.: "La protección de los datos personales ante el Tribunal Constitucional español", *Cuestiones Constitucionales. Revista Mexicana de Derecho Constitucional*, núm. 23, julio-diciembre 2010, pp. 3-25.
- AA.VV.: *La Europa de los Derechos. El Convenio Europeo de Derechos Humanos* (GARCÍA ROCA, J. y SANTAOLAYA MACHETTI, P. –coordinadores–), CEPC, Madrid, 2014, pp. 21-48.
- ÁLVAREZ CARO, M. y URIARTE LANDA, I.: "Dos visiones sobre la regulación de la privacidad y la innovación digital", *Expansión* (sección Jurídico), 12 de septiembre de 2014 [https://www.expansion.com/2014/09/12/juridico/1410542198.html]
- BALAGUER CALLEJÓN, F.: "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, Dykinson, Madrid, 2008, pp. 133-158.
- BENNETT, S. C.: "EU privacy shield: Practical implications for U.S. litigation", *Practical Lawyer*, núm. 62, 2016.
- BILBAO UBILLOS, J. M.: "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, Madrid, 2020, pp. 15-134.
- BUTLER, A.: "United States. Whither privacy shield in the Trump Era", *European Data Protection Law Review*, núm. 3, 2017, pp. 111-113.
- CARMONA CONTRERAS, A.: "El espacio europeo de los derechos fundamentales: de la Carta a las constituciones nacionales", *Revista Española de Derecho Constitucional*, núm. 7, CEPC, Madrid, 2016, pp. 13-40.

- CHANDER, A.: "Is Data Localization a Solution for Schrems II?", *Journal of International Economic Law*, núm. 23, 2020, pp. 771-784.
- COSTELLO, R. A.: "Schrems II: Everything is Illuminated?", *European Papers*, 2020, pp. 1045-1059.
- QUADRA-SALCEDO JANINI, T. DE LA: "El papel del Tribunal Constitucional y de los tribunales ordinarios en un contexto de tutela multinivel de los derechos fundamentales", *El Cronista del Estado Social y Democrático de Derecho*, núm. 53-54, 2015, pp. 34-59.
- FUENTES MÁIQUEZ, A.: "Comentario de la STJUE de 16 de Julio de 2020, C-311/18 (Schrems II)", *Revista de la Facultad de Derecho (ICADE)*, enero, 2021, pp. 1-10.
- GARCÍA-PERROTE MARTÍNEZ, I., y GABRIEL GARCÍA-MICÓ, T.: "Identidad, cesión de datos personales y la decisión Privacy Shield tras la STJUE Schrems II", *Indret: Revista para el Análisis del Derecho,* núm. 3, 2020, pp. 551-559.
- GELLMAN, B y POITRAS, L.: "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program", en *The Washington Post*, 7 de junio de 2013.
- GREENWALD, G.: "NSA collecting phone records of millions of Verizon customers daily", en *The Guardian*, jueves 6 de junio de 2013, [https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order].
- GREENWALD, G. y MACASKILL, E.: "NSA Prism program taps in to user data of Apple, Google and others", en *The Guardian*, 7 Junio 2013, [https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data].
- HOPKINS, N.: "UK gathering intelligence via covert NSA operation", en *The Guardian*, 7 Junio 2013, [https://www.theguardian.com/technology/2013/jun/07/uk-gathering-secret-intelligence-nsa-prism].
- LEFÉBURE, A.: *El Caso Snowden: así espía Estados Unidos al mundo*., Clave intelectual, Madrid, 2014.

- LÓPEZ AGUILAR, J.F.: "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-EUUU", *Teoría y Realidad Constitucional*, núm. 39, 2017, pp. 557–581.

- MALDONADO, E.: "Bridging the gap in transatlantic data protection", *Discussion Paper*, No. 4/20. Europa-Kolleg Hamburg, Institute for European Integration, [http://hdl.handle.net/10419/224928]

- MANGAS MARTÍN, A.: "Comentario al artículo 51", en *Carta de los Derechos Fundamentales de la Unión Europea: comentario artículo por artículo* (Dir.: Mangas Martín), Fundación BBVA, 2008, pp. 809-825.

- MARTÍNEZ MARTÍNEZ, R.: *Derecho y cloud computing*, Civitas, Pamplona, 2012.

- MIGUEL ASENSIO, P. A. DE: "Implicaciones de la declaración de invalidez del Escudo de Privacidad", *La Ley Unión Europea,* núm. 84, septiembre 2020, pp. 1-5.

- ROLDAN BARBERO, J.: "La Carta de los Derechos Fundamentales de la Unión Europea: su estatuto constitucional", *Revista de Derecho Comunitario Europeo*, núm. 16, septiembre-diciembre, 2003, pp. 943-991.

- RUIZ MIGUEL, C.: "El derecho a la protección de datos de carácter personal en la Carta de Derechos Fundamentales de la Unión Europea: Análisis crítico", *Revista de Derecho Comunitario Europeo*, núm. 14, enero-abril, 2003, pp. 7-43.

- SÁIZ ARNÁIZ, A.: "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 *Constitución europea y constituciones nacionales* [Gómez Fernández, I. (coord.)/Cartabia, M. (dir.)/De Witte, B. (dir.)/Pérez Tremps, P. (dir.)], Tirant lo Blanch, Valencia, 2005, pp. 531-588.

- SALAMANCA AGUADO, E.: "El respeto a la vida privada y a la protección de datos personales en el contexto de la vigilancia masiva de comunicaciones", *Revista del Instituto Español de Estudios Estratégicos,* núm. 4, 2014, pp. 151-177.

- TAPSCOTT, D.: *The digital economy: promise and peril in the age of networked intelligence*, New York: McGraw-Hill, 1997.

- TORRES VIÑALS, J.: *Del cloud computing al big data,* UOC (Universitat Operta de Catalunya), 2012.
- TRACOL, X.: "Schrems II: The return of the Privacy Shield", *Computer Law & Security Review,* núm. 39, 2020, [https://www.sciencedirect.com/science/article/abs/pii/S0267364920300893?dgcid=rss_sd_all&utm_campaign=RESR_MRKT_Researcher_inbound&utm_medium=referral&utm_source=researcher_app]
- TRONCOSO REIGADA, A.: *Comentarios al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales*, Cívitas, Pamplona, 2021.

B) SENTENCIAS

- STC 254/1993, de 20 de julio.
- STC 290/2000, de 30 de noviembre.
- STC 292/2000, de 30 de noviembre.
- STEDH de 17 de julio de 2003, Perry c. Reino Unido.
- STJUE de 16 de julio de 2020, Schrems (C-311/18,EU:C:2020:559).
- STJUE de 18 de octubre de 2016, Nikiforidis (C-135/15, EU:C:2016:774).
- STJUE de 2 de abril de 2020, Ruska Federacija (C-897/19 PPU, EU:C:2020:262).
- STJUE de 20 de marzo de 2018, Menci (C-524/15, EU:C:2018:197).
- STJUE de 26 de febrero de 2013, Akerberg Fransson (C-617/10, EU:C:2013:105).
- STJUE de 6 de octubre de 2015, Schrems (C-362/14,EU:C:2015:650).
- STJUE de 8 de abril de 2014, Comisión/Hungría (C-288/12, EU:C:2014:237).
- STJUE de 8 de abril de 2014, Digital Rights Ireland y otros (C-293/12 y C-594/12, EU:C:2014:238).
- STJUE de 9 de marzo de 2010, Comisión/Alemania (C-518/07, EU:C:2010:125).

C) DECISIONES DE LA COMISIÓN EUROPEA

- Decisión 2001/497/CE de la Comisión, de 15 de junio de 2001.
- Decisión 2004/915/CE de la Comisión, de 27 de diciembre de 2004, por la que se modifica la Decisión 2001/497/CE.

- Decisión 2010/87/UE de la Comisión, de 5 de febrero de 2010.
- Decisión de Ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016.

D) OTROS RECURSOS *ON-LINE*

- AUTORIDAD FEDERAL ALEMANA DE PROTECCIÓN DE DATOS (*DER BUNDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ UND DIE* INFORMATIONSFREIHEIT) [http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/89DSK-SafeHarbor.html?cms_sortOrder=score+desc&cms_templateQueryString=safe+harbor].
- COMISIÓN DE LIBERTADES CIVILES, JUSTICIA Y ASUNTOS DE INTERIOR DEL PARLAMENTO EUROPEO: *Informe sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU., los órganos de vigilancia en diversos Estados miembros y su impacto en los derechos fundamentales de los ciudadanos de la UE y en la cooperación transatlántica en materia de Justicia y Asuntos de Interior (2013/2188(INI)),* (A70139/2014) de 21 de febrero de 2014 [https://www.europarl.europa.eu/doceo/document/A-7-2014-0139_ES.pdf?redirect].
- COMISIÓN EUROPEA: *¿Qué son los datos personales?* [https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_es#:~:text=Los%20datos].
- COMITÉ EUROPEO DE PROTECCIÓN DE DATOS: *European Data Protection Board*) [https://edpb.europa.eu/edpb_es]
- COMITÉ EUROPEO DE PROTECCIÓN DE DATOS: *European Data Protection Board*), *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*, 24 de julio de 2020 [https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc311118_en.pdf]
- GREENWALD, G.; MacASKILL, E. y POITRAS, L.: "Edward Snowden: the whistleblower behind the NSA surveillance revelations", *The Guardian*, 11 de junio de 2013 [https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance]
- U.S. DEPARTMENT OF COMMERCE'S INTERNATIONAL TRADE ADMINISTRATION (ITA): *Export.Gov.* [http://export.gov/safeharbor/eu/eg_main_018496.asp].