Revista CESCO de Derecho de Consumo **Nº 15/2015**

http://www.revista.uclm.es/index.php/cesco **III. Noticias de Jurisprudencia**

TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES: ESTADOS UNIDOS NO ES UN PUERTO SEGURO, PERO TAMPOCO UNA ISLA INALCANZABLE[1]

STJUE (Gran Sala), de 6 de octubre de 2015, asunto C-362/14 (EU:C:2015:650)

Ana I. Mendoza Losana

Profesora de Derecho civil

Centro de Estudios de Consumo

Universidad de Castilla-La Mancha

El Tribunal de Justicia (Gran Sala) ha anulado la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos (Safe Harbour Decision) y ha declarado que las autoridades nacionales de control en materia de protección de datos son competentes, conforme al artículo 25.6 de la Directiva 95/46/CE, de protección de datos, para valorar, a instancia del titular de los datos, si un tercer Estado garantiza o no un nivel de protección adecuado de los datos personales cedidos y de los derechos fundamentales a la intimidad, aunque ya exista un pronunciamiento de la Comisión al respecto.

Además, de la sentencia se extraen las siguientes reglas que completan el régimen de protección de datos personales derivado del acervo comunitario:

1ª. Sólo se puede realizar una transferencia de datos personales a terceros países (fuera de la UE), si éstos garantizan un «nivel de protección adecuado» de los datos personales y de los derechos fundamentales reconocidos en la Carta de los Derechos Fundamentales de la Unión Europea.

2ª. "Nivel de protección adecuado" es un nivel de protección de las libertades y derechos fundamentales «sustancialmente equivalente al garantizado en la Unión por la Directiva 95/46, entendida a la luz de la Carta» (apdos. 73 y 74).

[1] Trabajo realizado en el marco del Programa Estatal de Fomento de la Investigación Científica y Técnica de Excelencia (Subprograma Estatal de Generación de Conocimiento) otorgado al Grupo de investigación y centro de investigación CESCO, *Mantenimiento y consolidación de una estructura de investigación dedicada al Derecho de consumo,* dirigido por el Prof. Ángel Carrasco Perera de la UCLM, Ref.: DER2014-5606-P.

3ª. Para llegar a un pronunciamiento sobre el carácter adecuado (o no) del nivel de protección concedido en terceros Estados, se ha de valorar periódicamente el contenido de las reglas aplicables en ese país, derivadas de la legislación interna o de los compromisos internacionales de éste, así como la práctica seguida para asegurar el cumplimiento de esas reglas, debiendo atender a todas las circunstancias relacionadas con una transferencia de datos personales a un tercer país (apdos. 75 y 76). No basta la valoración inicial, también se han de tener en cuenta las circunstancias sobrevenidas después de la adopción de una decisión (apdo. 77).

4ª. Los actos de las instituciones de la Unión gozan de una presunción de legalidad y por ello, producen efectos jurídicos mientras no hayan sido revocados, anulados en virtud de un recurso de anulación o declarados inválidos a raíz de una cuestión prejudicial o de una excepción de ilegalidad (sentencia Comisión/Grecia, C 475/01, EU:C:2004:585, apartado 18). También la Decisión 2000/520 de la Comisión que declara que un tercer Estado (EEUU) proporciona un nivel de protección adecuado a los datos personales goza de esa presunción de legalidad pero no impide el control por las autoridades nacionales a petición del titular de los datos.

5ª. Las funciones de control de la Comisión sobre las transferencias internacionales de datos de carácter personal concurren con las competencias de control de las autoridades nacionales. La Decisión de la Comisión no excluye la intervención de las autoridades nacionales. Toda autoridad nacional de control está investida 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 (apdos. 47 y 57 de la sentencia comentada). Aceptar que la decisión de la Comisión impide el pronunciamiento de las autoridades nacionales sobre las transferencias internacionales equivale a privar a las personas, cuyos datos hayan sido o pudieran ser transferidos al tercer país, del derecho garantizado por el artículo 8, apartados 1 y 3, de la Carta de presentar a las autoridades nacionales de control una solicitud para la protección de sus derechos fundamentales (véase, por analogía, la sentencia Digital Rights Ireland y otros, C 293/12 y C 594/12, EU:C:2014:238, apartado 68 y el apartado 58 de la sentencia comentada).

6ª. *Como cualquier acto de las instituciones comunitarias, las decisiones de la Comisión, dictadas al amparo del artículo 25.6 de la Directiva 95/46, están sometidos al control de su conformidad con los Tratados, con los principios generales del Derecho y con los derechos fundamentales (en ese sentido, además de la sentencia comentada, apdo. 60, las sentencias Comisión y otros/Kadi, C 584/10 P, C 593/10 P y C 595/10 P, EU:C:2013:518, apartado 66; Inuit Tapiriit Kanatami y otros/Parlamento y Consejo, C 583/11 P, EU:C:2013:625, apartado 91, y Telefónica/Comisión, C 274/12 P, EU:C:2013:852, apartado 56).*

7ª. *Sólo el TJUE puede declarar la nulidad de una Decisión de la Comisión: ni los tribunales nacionales, ni las autoridades de control en materia de protección de datos pueden declarar inválida la Decisión de la Comisión (sentencia comentada,*

apdo. 62 y sentencias Melki y Abdeli, C 188/10 y C 189/10, EU:C:2010:363, apartado 54, y CIVAD, C 533/10, EU:C:2012:347, apartado 40).

8ª. *La Decisión de la Comisión 2000/520 vulnera la Directiva 95/46 a la luz de la Carta de Derechos de la UE (apdo. 104 de la sentencia comentada) pues los principios de "puerto seguro" no garantizan una protección "adecuada" de los datos personales ni la salvaguarda de los derechos fundamentales de las personas por las siguientes razones: 1º) Porque las entidades adheridas se someten a un procedimiento de "autocertificación" que no permite identificar y sancionar las posibles vulneraciones de derechos fundamentales; 2º) Porque las entidades públicas estadounidenses no están sometidas a los principios de puerto seguro; 3º) Porque la aplicación de los principios de puerto seguro está limitada por la propia normativa de EEUU; 4º) Porque la Decisión 2000/520 reconoce la primacía de las «exigencias de seguridad nacional, interés público y cumplimiento de la ley [de Estados Unidos]» sobre los principios de puerto seguro y no exige justificación suficiente de las excepciones a la protección de los datos personales ni restringe la injerencia a lo estrictamente necesario; 5º) Porque la Decisión 2000/520 carece de mecanismos eficaces de protección ante eventuales injerencias en los derechos fundamentales.*

9ª. *Con todo y aunque el TJUE no lo expone porque no forma parte del objeto del litigio resuelto, en virtud del artículo 26.1,a de la Directiva 95/46, no sería necesario que la transferencia superara el control conforme al estándar "nivel adecuado de protección" si el propio titular de los datos consiente la transferencia*.

1. Supuesto de hecho: Facebook transfiere los datos personales cedidos en Europa a su filial en EEUU

Maximilian Schrems, estudiante de Derecho, nacional austriaco y residente en Austria, era usuario de la red Facebook desde 2008.

La práctica de Facebook exige que toda persona residente en el territorio de la Unión que desee utilizar la red social celebre en el momento de su inscripción un contrato con Facebook Ireland, filial de Facebook Inc., domiciliada ésta última en Estados Unidos. Los datos personales de los usuarios de Facebook Ireland residentes en el territorio de la Unión se transfieren en todo o en parte a servidores pertenecientes a Facebook Inc, situados en el territorio de Estados Unidos, donde son objeto de tratamiento.

El Sr. Schrems presentó ante la autoridad nacional de supervisión de protección de datos una reclamación en la que solicitaba que prohibiera a Facebook Ireland transferir sus datos personales a Estados Unidos. Alegaba que el Derecho vigente y las prácticas llevadas a cabo en ese país (actividades de vigilancia realizadas por las autoridades públicas) no garantizaban una protección suficiente de los datos personales conservados en su territorio. Como apoyo de esta reclamación, invocaba las revelaciones de Edward Snowden sobre las actividades de los servicios de información de Estados Unidos, en particular las de la National Security Agency («NSA») y otros organismos federales, como el Federal Bureau of Investigation (FBI).

La solicitud se rechazó por infundada. La autoridad nacional consideró que no había pruebas de que la NSA hubiera accedido a los datos personales del interesado y que cualquier cuestión referida al carácter adecuado de la protección de los datos personales en Estados Unidos debía resolverse conforme a la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes publicadas por el Departamento de Comercio de Estados Unidos de América (*Safe Harbour Decision*) (DO L 215, p. 7). En esta Decisión, la Comisión ya había constatado que Estados Unidos garantizaba un nivel adecuado de protección.

El particular interpone recurso contra la resolución ante un tribunal irlandés (*High Court*) que califica el recurso como una impugnación del régimen de «puerto seguro» establecido por la Decisión 2000/520 y eleva cuestión prejudicial ante el Tribunal de Justicia de la Unión Europea.

2. Cuestión prejudicial

En el contexto de la reclamación presentada ante la autoridad nacional en la que se afirma que se están transmitiendo datos personales a Estados Unidos, cuya legislación y práctica no garantizan una protección adecuada del titular de los datos, el tribunal irlandés plantea las siguientes cuestiones:

1. *¿Está vinculada la autoridad nacional 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 de los Derechos Fundamentales de la Unión Europea y no obstante lo dispuesto en el artículo 25, apartado 6, de la Directiva 95/46/CE?*

2. *En caso contrario, ¿puede o debe realizar la autoridad nacional su propia investigación del asunto a la luz de la evolución de los hechos que ha tenido lugar desde que se publicó por vez primera la Decisión 2000/520?*

En otros términos, se cuestiona si y en qué medida, 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 los datos personales que la conciernen, 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.

Sin perjuicio de la exposición detallada de los argumentos invocados por el TJUE, cabe adelantar que el TJUE contesta a las cuestiones planteadas que el

artículo 25.6 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 adoptada en virtud de la referida disposición, como la Decisión 2000/520, por la que la Comisión constata que un tercer país garantiza un nivel de protección adecuado, no impide que una autoridad de control de un Estado miembro, 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 éste no garantizan un nivel de protección adecuado (apdo. 66).

3. Régimen jurídico de las transferencias internacionales de datos de carácter personal

Antes de analizar el contenido de la sentencia, se han de exponer los rasgos generales del régimen de las transferencias internacionales en el marco de la normativa europea de protección de datos de carácter personal.

Se entiende por <transferencia internacional" aquella en la que los datos de carácter personal se ceden a una entidad pública o privada situada fuera del territorio de la Unión Europea. La operación consistente en transferir datos personales desde un Estado miembro a un tercer país constituye por sí misma un tratamiento de datos personales realizado en el territorio de un Estado miembro (v. apdo. 45 de la sentencia comentada y apdo. 56 de la sentencia Parlamento/Consejo y Comisión, C-317/04 y C-318/04), apdo. 45).

El régimen de las transferencias internacionales se regula en los artículos 25 y 26 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 (DO L 281, p. 31), en su versión modificada por el Reglamento (CE) nº 1882/2003 del Parlamento Europeo y del Consejo, de 29 de septiembre de 2003 (DO L 284, p. 1). Este régimen ha sido calificado como complementario al régimen general de protección del capítulo II, dirigido a garantizar un control por los Estados miembros de las transferencias de datos personales hacia terceros países (v. la sentencia Lindqvist, C 101/01, EU:C:2003:596, apartado 63).

3.1. «Nivel de protección adecuado»

Según el artículo 25.1 de la Directiva, la transferencia de datos personales sólo se puede realizar si los terceros países garantizan un «nivel de protección adecuado». En caso contrario, la transferencia debe prohibirse (cdo. 57 Directiva 95/46). El artículo 25.2 explica que «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».

El Derecho irlandés, -como el español y el de la Unión Europea en general-, prohíbe la transferencia de datos personales fuera del territorio nacional, excepto cuando el tercer país interesado asegura un nivel de protección adecuado de la vida privada y de los derechos y libertades fundamentales. La importancia de los derechos al respeto de la vida privada y a la inviolabilidad del domicilio, protegidos tanto por la Carta europea de Derechos Fundamentales como por las constituciones de los Estados miembros, exige que toda injerencia en esos derechos sea proporcionada y ajustada a las exigencias previstas por la ley.

Pero, ¿qué se entiende por «nivel de protección adecuado»? El TJUE pone de manifiesto que ni el artículo 25.2 de la Directiva 95/46 ni ninguna otra de sus disposiciones contienen una definición del concepto de «nivel de protección adecuado». En particular, el artículo 25.2 se limita a enunciar que el carácter adecuado del nivel de protección que ofrece un tercer país «se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos», y enumera sin carácter exhaustivo las circunstancias que se deben considerar en esa apreciación (apdo. 70 de la sentencia comentada). El artículo 25.6 de la Directiva exige que el país al que se transfieren los datos «garantice» un nivel de protección adecuado en razón de su legislación interna o de sus compromisos internacionales. El carácter adecuado del nivel de protección que ofrece un tercer país se ha de apreciar «a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas».

El TJUE concluye que "protección adecuada" en un tercer país es protección "sustancialmente equivalente" a la dada en la UE. Admite que el término «adecuado» que figura en el artículo 25.6 de la Directiva 95/46 significa que no cabe exigir que un tercer país garantice un nivel de protección idéntico al garantizado en el ordenamiento jurídico de la Unión. Sin embargo, «debe entenderse la expresión "nivel de protección adecuado" en el sentido de que exige que ese tercer país garantice efectivamente, por su legislación interna o sus compromisos internacionales, un nivel de protección de las libertades y derechos fundamentales sustancialmente equivalente al garantizado en la Unión por la Directiva 95/46, entendida a la luz de la Carta» (apdo. 73). Aunque los medios de los que se sirva ese tercer país para garantizar ese nivel de protección pueden ser diferentes de los aplicados en la Unión, deben ser eficaces en la práctica para garantizar una protección sustancialmente equivalente a la garantizada en la Unión" (apdo 74).

La Comisión (o la autoridad nacional) que valore si la protección conferida a los datos por un tercer Estado es "adecuada" está obligada a apreciar el contenido de las reglas aplicables en ese país, derivadas de la legislación

interna o de los compromisos internacionales de éste, así como la práctica seguida para asegurar el cumplimiento de esas reglas, debiendo atender a todas las circunstancias relacionadas con una transferencia de datos personales a un tercer país (apdo. 75 de la sentencia comentada).

El control sobre el nivel de protección exige una comprobación periódica sobre la persistencia de las normas y/ o de las prácticas que llevaron a valorar positivamente el nivel de protección dado a los datos personales, máxime si, como ocurre en el caso, hay indicios que generan dudas sobre el nivel de protección (apdo. 76 de la sentencia comentada). No basta la valoración inicial, también se han de tener en cuenta las circunstancias sobrevenidas después de la adopción de una decisión (apdo. 77 de la sentencia comentada).

3.2. ¿Quién valora el nivel de protección concedido por un tercer Estado? Coordinación Comisión y autoridades nacionales independientes

Del artículo 25 de la Directiva 95/46 resulta que la constatación de que un tercer país garantiza o no un nivel de protección adecuado pueden realizarla bien los Estados miembros o bien la Comisión. Con fundamento en el artículo 25. 6 de la Directiva 95/46, la Comisión puede adoptar una decisión que constate que un tercer país garantiza un nivel de protección adecuado. En ejercicio de esta potestad, la Comisión aprobó la citada Decisión 2000/520/CE en la que constató que Estados Unidos garantizaba un nivel adecuado de protección. La Comisión ha adoptado decisiones similares respecto a Argentina (Decisión 2003/490/CE), Andorra (Decisión 2010/625/UE), Israel (Decisión 2011/61/UE), Nueva Zelanda (Decisión 2013/65/UE) o Uruguay (Decisión 2012/484/UE), por citar sólo algunos.

Los Estados miembros deben adoptar las medidas necesarias para ajustarse a las decisiones de la Comisión.

Sin embargo, el TJUE afirma que las funciones de control de la Comisión sobre las transferencias internacionales de datos de carácter personal concurren con las competencias de control de las autoridades nacionales. El artículo 28 de la Directiva 95/46 obliga a los Estados miembros a disponer de autoridades públicas independientes que se encarguen de vigilar la aplicación en su territorio de las normas relativas a la protección de datos personales y conforme al artículo 8. 3 de la Carta de los derechos fundamentales de la UE, las autoridades nacionales de control están encargadas del control del cumplimiento de las reglas de la Unión para la protección de las personas físicas frente al tratamiento de datos personales. Se atribuyen a estas autoridades facultades de investigación, facultades de intervención, como la de prohibir provisional o definitivamente un tratamiento de datos, o la capacidad de comparecer en juicio. Todo ello respecto a los tratamientos de datos personales realizados en el territorio del Estado miembro de esas autoridades (no sobre los tratamientos de datos realizados en el territorio de un tercer país). Como declara la Directiva 95/46 (considerando 62) y ha destacado el TJUE

(sentencias Comisión/Alemania, C-518/07, EU:C:2010:125, apdo. 25, Comisión/Hungría C-288/12, EU:C:2014:237, apdo. 48 y la sentencia comentada, apdo. 47), la creación en los Estados miembros de autoridades de control independientes constituye un elemento esencial de la protección de las personas frente al tratamiento de datos personales.

Entre las diversas funciones atribuidas a estas entidades, «entenderá(n) de las solicitudes que cualquier persona, […], le presente en relación con la protección de sus derechos y libertades respecto del tratamiento de datos personales». En particular, entenderán «de las solicitudes de verificación de la licitud de un tratamiento que le presente cualquier persona cuando sean de aplicación las disposiciones nacionales…» (art. 28.4).

Por todo ello, el TJUE considera que la decisión de la Comisión no excluye la intervención de estas autoridades. Toda autoridad nacional de control está investida 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, aunque la Comisión ya se hubiera pronunciado (apdo. 47 de la sentencia comentada). En este contexto, se hace necesario diseñar mecanismos para coordinar las funciones de la Comisión y de las autoridades nacionales.

Los actos de las instituciones de la Unión disfrutan en principio de una presunción de legalidad, y producen por tanto efectos jurídicos mientras no hayan sido revocados, anulados en virtud de un recurso de anulación o declarados inválidos a raíz de una cuestión prejudicial o de una excepción de ilegalidad (sentencia Comisión/Grecia, C 475/01, EU:C:2004:585, apartado 18 y la jurisprudencia citada). Correlativamente, también la Decisión de la Comisión 2000/520 goza de la presunción de legalidad pero no impide el control por las autoridades nacionales a petición del titular de los datos. En virtud del artículo 288 TFUE, párrafo cuarto, la citada decisión de la Comisión tiene carácter obligatorio para todos los Estados miembros destinatarios y vincula a todos sus órganos (sentencias Albako/BALM, 249/85, EU:C:1987:245, apartado 17, y Mediaset, C 69/13, EU:C:2014:71, apartado 23), en cuanto tiene el efecto de autorizar transferencias de datos personales desde los Estados miembros al tercer país al que se refiere dicha decisión. Mientras la decisión de la Comisión no haya sido declarada inválida por el Tribunal de Justicia, los Estados miembros y sus órganos, entre ellos las autoridades de control independientes, no pueden adoptar medidas contrarias a esa decisión, como serían actos por los que se apreciara con efecto obligatorio que el tercer país al que se refiere dicha decisión no garantiza un nivel de protección adecuado.

Con todo, una decisión de la Comisión adoptada en virtud del artículo 25.6 de la Directiva 95/46, como la Decisión 2000/520, no puede impedir que las personas cuyos datos personales hayan sido o pudieran ser transferidos a un tercer país presenten a las autoridades nacionales de control una solicitud, prevista en el artículo 28.4 de la Directiva 95/46, para la protección de sus derechos y libertades frente al tratamiento de esos

datos. De igual forma, una decisión de esa naturaleza no puede dejar sin efecto ni limitar las facultades expresamente reconocidas a las autoridades nacionales de control por el artículo 8.3 de la Carta y por el artículo 28 de la referida Directiva. Ni el artículo 8, apartado 3, de la Carta, ni el artículo 28 de la Directiva 95/46 excluyen del ámbito de la competencia de las autoridades nacionales designadas a ese efecto el control de las transferencias de datos personales a terceros países a los que se refiera una decisión de la Comisión en virtud del artículo 25, apartado 6, de esa Directiva. En particular, el artículo 28.4, párrafo primero, de la Directiva 95/46, que dispone que las autoridades nacionales de control entenderán de la solicitud que presente «cualquier persona […] en relación con la protección de sus derechos y libertades respecto del tratamiento de datos personales», no prevé ninguna excepción en ese sentido, en el supuesto de que la Comisión hubiera adoptado una decisión en virtud del artículo 25, apartado 6, de esa Directiva.

Además, sería contrario al sistema establecido por la Directiva 95/46 y a la finalidad de sus artículos 25 y 28 que una decisión de la Comisión adoptada en virtud del artículo 25.6 de dicha Directiva tuviera el efecto de impedir que una autoridad nacional de control examine la solicitud de una persona para la protección de sus derechos y libertades frente al tratamiento de sus datos personales que hayan sido o pudieran ser transferidos desde un Estado miembro a un tercer país al que se refiere esa decisión de la Comisión.

3.3. Excepciones

El artículo 26 de la Directiva 95/46 admite ciertas excepciones al principio de «nivel de protección adecuado». Entre otras, los Estados miembros dispondrán que pueda efectuarse una transferencia de datos personales a un país tercero que no garantice un nivel de protección adecuado «siempre y cuando el interesado haya dado su consentimiento inequívocamente a la transferencia prevista» (art. 26.1.*a* Directiva).

El consentimiento del interesado excluye el control sobre el carácter adecuado de la protección concedida en terceros Estados. Aquellos organismos o empresas que pretendan transferir datos desde la Unión Europea a Estados Unidos (o a cualquier otro Estado fuera de la UE) sin pasar por el control de la Comisión o de las autoridades nacionales de control deberán requerir el consentimiento de los interesados. En virtud del inexcusable principio de calidad de los datos (art. 6 Directiva), dicho consentimiento debe ser un consentimiento informado, es decir, se habría de facilitar información completa sobre el destino de los datos, los derechos de acceso, rectificación, cancelación u oposición o en su caso, la inexistencia de los mismos y sobre las medidas de protección de datos adoptadas en el país de destino (arts. 7.*a* y 10 Directiva).

4. La Decisión de la Comisión 2000/520 vulnera la Directiva 95/46 a la luz de la Carta de derechos fundamentales de la UE

4.1. Extralimitación competencial de la Comisión

La Decisión 2000/520 de la Comisión impide a las autoridades nacionales independientes ejercer las funciones que la Directiva les atribuye. Así, el artículo 3.1, párrafo primero, de la Decisión 2000/520 establece una regulación específica de las facultades de las que disponen las autoridades nacionales de control ante una constatación realizada por la Comisión sobre el nivel de protección adecuado. Según destaca el TJUE, «sin perjuicio de sus facultades para emprender acciones que garanticen el cumplimiento de las disposiciones nacionales adoptadas de conformidad con disposiciones diferentes del artículo 25 de la Directiva [95/46], […], las referidas autoridades podrán ejercer su facultad de suspender los flujos de datos hacia una entidad que haya autocertificado su adhesión a los principios [de la Decisión 2000/520] de manera restrictiva, ya que sólo es posible la intervención a partir de un alto umbral de condiciones» (apdo. 101 de la sentencia comentada). Esta disposición no enerva las facultades de esas autoridades para tomar medidas encaminadas a asegurar el cumplimiento de las disposiciones nacionales adoptadas en aplicación de la Directiva, pero sí excluye la posibilidad de que esas autoridades tomen medidas con objeto de asegurar el cumplimiento del artículo 25 de la misma Directiva. Por tanto, el artículo 3, apartado 1, párrafo primero, de la Decisión 2000/520 debe entenderse en el sentido de que priva a las autoridades nacionales de control de las facultades que les atribuye el artículo 28 de la Directiva 95/46, en el supuesto de que una persona alegue, con ocasión de una solicitud basada en esa disposición, factores que puedan afectar a la compatibilidad de una decisión de la Comisión, adoptada conforme al artículo 25.6 de esa directiva, según la que un tercer país garantiza un nivel de protección adecuado con la protección de la vida privada y de las libertades y derechos fundamentales de las personas.

Sin embargo, la facultad atribuida a la Comisión por el legislador de la Unión en el artículo 25.6 de la Directiva 95/46 no le confiere la competencia para restringir las facultades de las autoridades nacionales de control. Al contrario, el TJUE considera que aceptar que la decisión de la Comisión impide el pronunciamiento de las autoridades nacionales sobre las transferencias internacionales, equivale a privar a las personas, cuyos datos hayan sido o pudieran ser transferidos al tercer país, del derecho de presentar a las autoridades nacionales de control una solicitud para la protección de sus derechos fundamentales garantizados por el artículo 8, apartados 1 y 3 de la Carta (por analogía, la sentencia *Digital Rights Ireland* y otros, C-293/12 y C-594/12, EU:C:2014:238, apartado 68 y el apartado 58 de la sentencia comentada).

Por todo ello, concluye el TJUE que al adoptar el artículo 3 de la Decisión 2000/520, la Comisión excedió los límites de la competencia que

le atribuye el artículo 25, apartado 6, de la Directiva 95/46, entendido a la luz de la Carta, y que dicho artículo 3 es inválido (apdo. 104).

4.2. Los derechos fundamentales como límites al control de la Comisión

Como en anteriores sentencias, el TJUE fundamenta su intervención en la necesidad de tutelar el derecho fundamental al respeto de la vida privada garantizado por el artículo 7 de la Carta y el derecho fundamental a la protección de los datos personales que garantiza el artículo 8 de ésta (sentencias *Rijkeboer*, C-553/07, EU:C:2009:293, apartado 47; *Digital Rights Ireland* y otros, C-293/12 y C-594/12, EU:C:2014:238, apartado 53, y *Google Spain y Google*, C-131/12, EU:C:2014:317, apartados 53, 66 y 74 y la jurisprudencia citada).

El conflicto que en principio se presenta como una solicitud particular de tutela del derecho a la protección de datos planteada ante una autoridad nacional acaba convertido en un análisis de la compatibilidad de la Decisión 2000/25 de la Comisión con la protección de la vida privada y de las libertades y derechos fundamentales de las personas.

Las decisiones de la Comisión, como el resto del Derecho comunitario, están sometidas a los derechos fundamentales. La Unión es una Unión de Derecho en la que todos los actos de sus instituciones están sujetos al control de su conformidad, en particular, con los Tratados, con los principios generales del Derecho y con los derechos fundamentales (en ese sentido, además de la sentencia comentada, apdo. 60, las sentencias Comisión y otros/Kadi, C-584/10 P, C-593/10 P y C-595/10 P, EU:C:2013:518, apartado 66; *Inuit Tapiriit Kanatami* y otros/Parlamento y Consejo, C-583/11 P, EU:C:2013:625, apartado 91, y Telefónica/Comisión, C-274/12 P, EU:C:2013:852, apartado 56). Por tanto, las decisiones de la Comisión adoptadas en virtud del artículo 25.6 de la Directiva 95/46 no pueden quedar excluidas de ese control.

La facultad de apreciación de la Comisión sobre el carácter adecuado del nivel de protección garantizado por un tercer país queda condicionada a un control estricto de las exigencias derivadas del artículo 25 de la Directiva 95/46, entendido a la luz de la Carta (apdo. 78 se la sentencia comentada y la sentencia *Digital Rights Ireland* y otros, C-293/12 y C-594/12, EU:C:2014:238, apartados 47 y 48).

Como se ha dicho, la Decisión supone una extralimitación de la Comisión en cuanto priva a las autoridades nacionales de control de realizar funciones que la Directiva de protección de datos les atribuye. Independientemente del fondo de la cuestión, desde el punto de vista procedimental, aceptar que la decisión de la Comisión impide el pronunciamiento de las autoridades nacionales sobre las transferencias internacionales equivale a privar a las personas, cuyos datos hayan sido o pudieran ser transferidos al tercer país, del derecho de presentar a las autoridades nacionales de control una solicitud para la protección de sus

derechos fundamentales garantizado por el artículo 8, apartados 1 y 3 de la Carta (por analogía, la sentencia *Digital Rights Ireland* y otros, C-293/12 y C-594/12, EU:C:2014:238, apartado 68 y el apartado 58 de la sentencia comentada).

4.3. La Comisión no valoró correctamente el nivel de protección concedido a los datos personales

En palabras del TJUE, «la Comisión no manifestó en la Decisión 2000/520 que Estados Unidos "garantiza" efectivamente un nivel de protección adecuado en razón de su legislación interna o sus compromisos internacionales» (apdo. 97). Por lo que el Tribunal concluye que «el artículo 1 de esa Decisión vulnera las exigencias establecidas por el artículo 2.6 de la Directiva 95/46, entendido a la luz de la Carta, y es inválido por esa causa» (apdo. 98).

No cabe argumentar que la Comisión no se percató de la falta de garantías de protección de los derechos cedidos a Estados Unidos. Al contrario, la apreciación que la misma Comisión realizó sobre la situación resultante de la aplicación de esa Decisión plasmada en los puntos 2 y 3.2 de la Comunicación al Parlamento Europeo y al Consejo titulada «Restablecer la confianza en los flujos de datos entre la UE y EE.UU» [COM(2013) 846 final] y en los puntos 7.1, 7.2 y 8 de la Comunicación al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE [COM(2013) 847], revela que la Comisión constató que las autoridades estadounidenses podían acceder a los datos personales transferidos por los Estados miembros a Estados Unidos y tratarlos de manera incompatible con las finalidades de esa transferencia, que excedía de lo que era estrictamente necesario y proporcionado para la protección de la seguridad nacional. De igual modo, la Comisión apreció que las personas afectadas no disponían de vías jurídicas administrativas o judiciales que les permitieran acceder a los datos que les concernían y obtener, en su caso, su rectificación o supresión.

Independientemente de la invalidación de la Decisión 2000/520, cabría reprochar a la Comisión el incumplimiento de la Directiva comunitaria de protección de datos en cuanto no garantizó la adecuada protección de los datos y exigir la correspondiente responsabilidad por las eventuales injerencias en los derechos fundamentales acaecidas en el marco de la decisión. Naturalmente, para demostrar la existencia de una injerencia en el derecho fundamental al respeto de la vida privada carece de relevancia que la información relativa a la vida privada de que se trate tenga o no carácter sensible o que los interesados hayan sufrido o no inconvenientes en razón de tal injerencia (apdo. 87 de la sentencia comentada y sentencia *Digital Rights Ireland* y otros, C 293/12 y C 594/12, EU:C:2014:238, apartado 33 y la jurisprudencia citada).

4.4. Sólo el TJUE puede declarar la nulidad de una Decisión de la Comisión: ni los tribunales nacionales, ni las autoridades de control en materia de protección de datos pueden declarar inválida la Decisión de la Comisión

El TJUE destaca que la competencia para declarar la invalidez de un acto de la Unión como una decisión de la Comisión adoptada en virtud del artículo 25.6 de la Directiva 95/46 corresponde en exclusiva al propio Tribunal (apdo. 62 sentencia comentada y sentencias *Melki y Abdeli*, C 188/10 y C 189/10, EU:C:2010:363, apartado 54, y CIVAD, C 533/10, EU:C:2012:347, apartado 40). Admite que los tribunales nacionales están facultados para examinar la validez de un acto de la Unión, como una decisión de la Comisión adoptada en virtud del artículo 25.6 de la Directiva 95/46, pero carecen de competencia para declarar su invalidez (*vid*. las sentencias *Foto-Frost*, 314/85, EU:C:1987:452, apartados 15 a 20, e IATA y ELFAA, C-344/04, EU:C:2006:10, apartado 27)". *A fortiori*, tampoco las autoridades nacionales de control están habilitadas para declarar la invalidez de la referida Decisión (apdo. 62 sentencia comentada) pero sí para pronunciarse sobre la solicitud del particular titular de los datos.

El Tribunal detalla el procedimiento que se ha de seguir en caso de que la autoridad nacional considere infundada la denuncia del particular afectado (apdo. 64). Así, si la citada autoridad considera que los datos alegados en apoyo de esa solicitud son infundados y la desestima, la persona que haya presentado la solicitud debe disponer de recursos jurisdiccionales que le permitan impugnar esa decisión lesiva para ella ante los tribunales nacionales, que están obligados a suspender el procedimiento y plantear al Tribunal de Justicia una cuestión prejudicial de validez si estiman que uno o varios de los motivos de invalidez alegados por las partes o, en su caso, suscitados de oficio son fundados (véase, en ese sentido, la sentencia *T & L Sugars y Sidul Açúcares/Comisión,* C 456/13 P, EU:C:2015:284, apartado 48 y jurisprudencia citada).

5. ¿Por qué los principios de «puerto seguro» a los que se refiere la Decisión 2000/520 no garantizan una protección «adecuada» de los datos personales?

Aunque sin entrar a valorar los principios de «puerto seguro» a los que se refiere la Decisión, el TJUE ya concluye que ésta vulnera las exigencias del artículo 25.6 de la Directiva 95/46 a la luz de la Carta (apdo. 98), el Tribunal también se pronuncia sobre el nivel de protección concedido por tales principios llegando igualmente a la conclusión de que no ofrecen el nivel de protección adecuado por las siguientes razones:

1º. *Porque las entidades adheridas se someten a un procedimiento de «autocertificación» que no permite identificar y sancionar las posibles vulneraciones de derechos fundamentales.* La adhesión de una entidad a los principios de puerto seguro se lleva a cabo conforme a un sistema de autocertificación, como resulta del artículo 1, apartados 2 y 3, de esa Decisión, en relación con la FAQ nº 6 que figura en su anexo II. La fiabilidad

de ese sistema en relación con la exigencia del nivel de protección adecuada descansa, en esencia, en el establecimiento de mecanismos eficaces de detección y de control que permitan identificar y sancionar en la práctica las posibles infracciones de las reglas que garantizan la protección de los derechos fundamentales, en especial del derecho al respeto de la vida privada y del derecho a la protección de los datos personales. No se constata la existencia de estos mecanismos.

2º. *Porque las entidades públicas estadounidenses no están sometidas a los principios de puerto seguro.* Sólo quedan sometidas a dichos principios las entidades adheridas autocertificadas.

3º. *Porque la aplicación de los principios de puerto seguro está limitada por la propia normativa de EEUU*. Si la legislación estadounidense establece una obligación en contrario, las entidades deben cumplirla, dentro o fuera del ámbito de los principios de puerto seguro (título B de su anexo IV la Decisión 2000/520). El Tribunal pone de manifiesto que la Decisión 2000/520 no contiene ninguna constatación sobre la existencia en Estados Unidos de reglas estatales destinadas a limitar las posibles injerencias en los derechos fundamentales de las personas cuyos datos se transfieran desde la Unión a Estados Unidos, injerencias que estuvieran autorizadas a llevar a cabo entidades estatales de ese país cuando persigan fines legítimos, como la seguridad nacional.

En particular, el TJUE declara que «se debe considerar que una normativa que permite a las autoridades públicas acceder de forma generalizada al contenido de las comunicaciones electrónicas lesiona el contenido esencial del derecho fundamental al respeto de la vida privada garantizado por el artículo 7 de la Carta» (apdo. 94 de la sentencia comentada y la sentencia *Digital Rights Ireland* y otros, C-293/12 y C-594/12, EU:C:2014:238, apartado 39).

Una normativa que haga posible una injerencia 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 una medida e impongan unas exigencias mínimas, de modo 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 ellos (sentencia *Digital Rights Ireland* y otros, C-293/12 y C-594/12, EU:C:2014:238, apartados 54 y 55 y la jurisprudencia citada).

De igual manera, una normativa que no prevé posibilidad alguna de que el justiciable ejerza acciones en Derecho para acceder a los datos personales que le conciernen o para obtener su rectificación o supresión no respeta el contenido esencial del derecho fundamental a la tutela judicial efectiva que reconoce el artículo 47 de la Carta (apdo. 95).

4º. *Porque la Decisión 2000/520 reconoce la primacía de las «exigencias de seguridad nacional, interés público y cumplimiento de la ley [de Estados Unidos]» sobre los principios de puerto seguro*. Precisamente en virtud de esta primacía, las entidades estadounidenses autocertificadas que reciban datos personales desde la Unión están obligadas sin limitación a dejar de aplicar esos principios cuando éstos entren en conflicto con esas exigencias y se manifiesten incompatibles con ellas. Dado el carácter general de la excepción prevista en el anexo I, párrafo cuarto, de la Decisión 2000/520, ésta hace posibles injerencias en los derechos fundamentales de las personas, cuyos datos personales se transfieren o pudieran transferirse desde la Unión a Estados Unidos, fundadas en exigencias concernientes a la seguridad nacional, el interés público y el cumplimiento de la ley de Estados Unidos.

No se exige suficiente justificación en lo que atañe al nivel de protección de las libertades y derechos fundamentales garantizado en la Unión. Como en sentencias anteriores, el TJUE recuerda que las disposiciones de la Directiva 95/46, en cuanto regulan el tratamiento de datos personales, que puede vulnerar las libertades fundamentales y, en particular, el derecho al respeto de la vida privada, deben ser necesariamente interpretadas a la luz de los derechos fundamentales protegidos por la Carta (apdo. 38 de la sentencia comentada y sentencias *Österreichischer Rundfunk* y otros, C 465/00, C 138/01 y C 139/01, EU:C:2003:294, apartado 68; *Google Spain y Google*, C 131/12, EU:C:2014:317, apartado 68, y *Ryneš,* C 212/13, EU:C:2014:2428, apartado 29).

La protección del derecho fundamental al respeto de la vida privada al nivel de la Unión exige que las excepciones a la protección de los datos personales y las limitaciones de esa protección no excedan de lo estrictamente necesario (sentencia *Digital Rights Ireland* y otros, C 293/12 y C 594/12, EU:C:2014:238, apartado 52 y la jurisprudencia citada). Sin embargo, en el caso analizado "no se limita a lo estrictamente necesario una normativa que autoriza de forma generalizada la conservación de la totalidad de los datos personales de todas las personas cuyos datos se hayan transferido desde la Unión a Estados Unidos, sin establecer ninguna diferenciación, limitación o excepción en función del objetivo perseguido y sin prever ningún criterio objetivo que permita circunscribir el acceso de las autoridades públicas a los datos y su utilización posterior a fines específicos, estrictamente limitados y propios para justificar la injerencia que constituyen tanto el acceso a esos datos como su utilización [apdo. 93 de la sentencia comentada y acerca de 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 (*DO* L 105, p. 54), la sentencia *Digital Rights Ireland* y otros, C 293/12 y C 594/12, EU:C:2014:238, apartados 57 a 61].

5º. *Porque la Decisión 2000/520 carece de mecanismos eficaces de protección ante eventuales injerencias en los derechos fundamentales.* La Decisión

2000/520 no pone de manifiesto la existencia de una protección jurídica eficaz contra injerencias de la naturaleza descrita. Los mecanismos de arbitraje privado y los procedimientos ante la Comisión Federal de Comercio, cuyas facultades, descritas en particular en las FAQ nº 11 que figuran en el anexo II de esa Decisión, se limitan a los litigios comerciales, atañen al cumplimiento por las empresas estadounidenses de los principios de puerto seguro, y no se pueden aplicar en litigios concernientes a la legalidad de injerencias en los derechos fundamentales derivadas de medidas de origen estatal.

6. ¿Cuál será la estrategia de las empresas a partir de la sentencia *Schrems*?

Sin perjuicio de que la Comisión extreme las cautelas y sea más exigente en la valoración del nivel de protección de los datos personales concedido en terceros Estados o de que las autoridades nacionales aproximen sus criterios de actuación, cabe vaticinar que a partir de ahora, las empresas centrarán su estrategia en recabar el consentimiento de los interesados (art. 26.2 Directiva 95/46).

Ciertamente, ello podría hacer algo más lento el proceso en cuanto aquellos organismos o empresas que pretendan transferir datos desde la Unión Europea a Estados Unidos (o a cualquier otro Estado fuera de la UE) sin pasar por el control de la Comisión o de las autoridades nacionales de control deberán requerir el consentimiento de los interesados. En virtud del inexcusable principio de calidad de los datos (art. 6 Directiva), dicho consentimiento debe ser un consentimiento informado, es decir, se habría de facilitar información completa sobre el destino de los datos, los derechos de acceso, rectificación, cancelación u oposición o, en su caso, la inexistencia de los mismos y sobre las medidas de protección de datos adoptadas en el país de destino (arts. 7.*a* y 10 Directiva).

Con todo, es muy probable que la sentencia no suponga, -como se ha dicho-, ni el fin, ni la reducción de las transferencias internacionales de datos pues el interesado que quiera ser usuario de la red social en cuestión o del buscador de su interés sólo podrá acceder a tales servicios si acepta la política de privacidad de la empresa, que en su caso, incluya la transferencia de datos a terceros Estados, en los que el nivel de protección no sea sustancialmente idéntico al concedido en el ámbito de la Unión Europea.