La transcendencia práctica del caso Facebook en relación con la transferencia masiva de datos personales desde la Unión Europea a Estados Unidos

Practical Implication of Facebook Ruling on the large-scale Personal Data Transfer from the EU to the USA

Alicia Chicharro Lázaro – Universidad Pública de Navarra –
alicia.chicharro@unavarra.es

Abstract: Las normas europeas sobre protección de datos personales cumplen un papel crucial en relación con el derecho fundamental al respeto a la vida privada. Esas normas permiten la transferencia de este tipo de datos a terceros países fuera de la UE siempre que los mismos garanticen un nivel de protección adecuado.

Aunque estas transmisiones de datos tanto a autoridades públicas, como a empresas privadas de Estados Unidos, siempre han resultado polémicas, la desconfianza aumentó de forma exponencial a partir de la revelación de la existencia en ese país de varios programas de vigilancia que comprendían la recogida y el tratamiento de información a gran escala.

Por un lado, la sentencia del Tribunal de Justicia en el caso Facebook invalida la decisión adoptada por la Comisión en la que, apoyándose en el régimen de puerto seguro, consideraba que la legislación estadounidense garantizaba un nivel adecuado de protección de los datos personales transferidos desde la Unión a entidades establecidas en Estados Unidos.

Por el otro, el fallo clarifica los poderes de las autoridades nacionales de control ante solicitudes presentadas por ciudadanos europeos 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, aunque exista una decisión de la Comisión que autorice dichas transmisiones.

En definitiva, el Tribunal de Justicia reafirma la importancia de la intimidad y la protección de datos, derechos fundamentales que deben gozar de las mayores garantías posibles tanto en territorio europeo, como en caso de transferencia a terceros países.

Keywords: Datos personales; privacidad; derecho a la intimidad; redes sociales; autoridades nacionales de control

1. Introducción

La transferencia masiva de datos de carácter personal de ciudadanos europeos tanto a las autoridades públicas, como a las empresas privadas de Estados Unidos siempre ha estado rodeada de polémica. La protección del derecho a la intimidad y a la privacidad desarrollada por la legislación europea y adoptada internamente en cada uno de los Estados miembros se esgrime como paradigma de aptitud para la protección de los datos personales de los ciudadanos europeos no sólo en la Unión, sino también en las transferencias de los mismos a terceros países.

Revelaciones de tratamiento masivo de esos datos como las que formuló Edward Snowden[1], llevan a preguntarse si aquello que protegemos tan celosamente con nuestra normativa europea a nivel interno de la Unión, se ve despojado de la mayor parte de sus garantías cuando se transmite a las empresas o autoridades estadounidenses.

[1] A través del programa PRISM, la Agencia de Seguridad Nacional de Estados Unidos (NSA) vigilaba electrónicamente a los usuarios europeos de compañías como Facebook, Google, Yahoo, Dropbox, Apple o Microsoft. Los datos que supuestamente la NSA es capaz de obtener gracias a PRISM incluyen correos electrónicos, videos, chat de voz, fotos, direcciones IP, notificaciones de inicio y fin de sesión, transferencia de archivos y detalles de perfiles de las redes sociales.

La piedra angular de la normativa sobre protección de datos en la UE es la Directiva 95/46/CE[2]. Esta Directiva dispone que en principio solo se pueden transferir dichos datos a un país tercero si éste garantiza un nivel de protección adecuado. Así, la Comisión puede declarar que un Estado fuera de la Unión asegura de una forma correcta los datos personales, atendiendo a sus normas internas o a los instrumentos internacionales para los que ha prestado su consentimiento en obligarse. Basándose en una serie de principios a los que las empresas estadounidenses pueden adherirse voluntariamente y que se han venido en llamar programa o régimen de "puerto seguro"[3], la Comisión dictó la Decisión 2000/520/CE[4], afirmando que las transferencias de datos personales desde la Unión a Estados Unidos cumplían las salvaguardas contenidas en la Directiva 95/46/CE.

Sin embargo, el pasado 6 de octubre de 2015, el Tribunal de Justicia de la Unión Europea (TJUE) dictó una trascendente sentencia en la que declaró inválida dicha Decisión[5]. La petición de dictamen prejudicial tenía por objeto la interpretación de los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea y los artículos 25.6 y 28 de la Directiva sobre protección de datos.

Lo cierto es que los flujos masivos de datos de carácter personal hacia empresas como Facebook, Twitter o Google, cuyas sedes centrales se encuentran en territorio americano, son regulares. Estas transferencias afectan a un gran número de personas, cuyos derechos fundamentales pueden verse vulnerados, pero además a una gran cantidad de datos personales.

[2] Directiva 95/46/CE, 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), modificada por el Reglamento (CE) 1882/2003 (DO L 284, p. 1.

[3] US-EU Safe Harbor Overview, obtenido de <http:export.gov/safeharbor/eu/eg_main_018476.asp> (última consulta 15 octubre 2015). El régimen de puerto seguro incluye una serie de principios relativos a la protección de datos personales a los que las empresas estadounidenses pueden suscribirse voluntariamente. Tanto los principios como las preguntas más frecuentes (FAQ), en las que se proporciona orientación para aplicar los principios, fueron publicados por el Gobierno de Estados Unidos con fecha 21 de julio de 2000 y aparecen como anexos de la Decisión 2000/520/CE.

[4] Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América (DO L 215, p. 7).

[5] STJUE, 6 de octubre de 2015, Maximillian Schrems y Data Protection Commissioner, C-362/14, EU:C:2015:650.

ISBN-13: 978-84-16458-45-5 / D.L.: TF-162-2016 / DOI: 10.4185/cac103

Tanto la Unión como los Estados miembros tienen la obligación de garantizar a los ciudadanos europeos una protección eficaz de sus datos de carácter personal, incluso en el caso de que los mismos se transmitan a terceros países. Por ello, los posibles abusos que se puedan cometer deben ser oportunamente investigados, comprobados y, en su caso, sancionados, restableciéndose inmediatamente el nivel de protección que garantiza el Derecho de la Unión.

2. Antecedentes

El Tribunal de Justicia recibió una petición de decisión prejudicial en la que se le solicitaba interpretar diversos preceptos de la Carta de los Derechos Fundamentales de la UE y de la Directiva 95/46/CE, a la luz de los cuales debía analizar la validez de la Decisión 2000/520/CE por la que la Comisión daba el visto bueno a las transferencias de datos de carácter personal a empresas estadounidenses que autocertificasen, conforme al régimen de puerto seguro, una protección adecuada de los mismos.

El caso traía causa de una denuncia de Maximillian Schrems, un ciudadano austriaco usuario de Facebook desde 2008, cuyos datos personales, como ocurre con los demás usuarios que residen en la UE, se transfieren total o parcialmente desde la filial irlandesa de dicha red social (Facebook Ireland Ltd) a servidores situados en territorio de los Estados Unidos (Facebook Inc.), donde son conservados y objeto de tratamiento.

Schrems presentó una reclamación ante la Comisaria para la Protección de Datos irlandesa[6], la autoridad nacional de control. Según el demandante, a la luz de las revelaciones realizadas en 2013 por Edward Snowden en relación con las actividades de los servicios de información de Estados Unidos (en particular, la National Security Agency o NSA), la normativa y la práctica de este país no garantizaban una protección suficiente de los datos que se le transferían frente a las actividades de vigilancia por las autoridades públicas (Brown 2015: 23). La Comisaria para la Protección de Datos desestimó esa reclamación apreciando que en su Decisión 2000/520/CE la Comisión había

[6] Data Protection Commissioner, el cargo lo ostenta en este momento Helen Dixon.

ISBN-13: 978-84-16458-45-5 / D.L.: TF-162-2016 / DOI: 10.4185/cac103

constatado que, en el marco del régimen denominado de puerto seguro, Estados Unidos garantizaba un nivel adecuado de protección de los datos personales transferidos.

La defensa de Schrems apeló al Tribunal Supremo de Irlanda que, una vez examinadas las pruebas presentadas por las partes, concluyó que la vigilancia electrónica y la interceptación de los datos personales transmitidos desde la Unión a Estados Unidos servían a finalidades necesarias e indispensables para el interés público[7]. Sin embargo, tomando en consideración las revelaciones del Sr. Snowden, quedaba patente que la NSA y los organismos federales habían cometido "importantes excesos"[8].

Y son precisamente esos "excesos" los que siembran serias dudas acerca de la pertinencia del nivel de protección estadounidense de los datos personales, tanto conforme a la legislación irlandesa, como en relación con el Derecho de la Unión.

Por lo que se refiere a la legislación irlandesa, el acceso masivo e indiferenciado a los datos personales es manifiestamente contrario al principio de proporcionalidad y a los valores fundamentales protegidos por la Constitución. La transferencia de datos fuera del territorio nacional está prohibida, salvo cuando el tercer país asegura un nivel de protección adecuado de los datos personales y del derecho a la vida privada. Ante las sospechas fundadas que plantea el sistema de Estados Unidos, la Comisaria debería haber investigado la reclamación del Sr. Schrems, en vez de desestimarla directamente.

Así mismo, el Alto Tribunal irlandés considera que el asunto atañe a la aplicación del Derecho de la Unión y que la legalidad de la decisión discutida en el asunto principal debe apreciarse a la luz de esa legislación. Según este órgano judicial, la Decisión 2000/520/CE no se ajusta a las exigencias

[7] El propio Tribunal Supremo irlandés ya aludió a una justificación específica adecuada para esta clase de vigilancia que "es capaz de afectar gravemente a la tranquilidad y a la reputación pública de cada individuo"; Irish High Court, Kane v. Governor of Mountjoy Prison, 1988, IR 757 769.

[8] En relación con la cantidad de datos que la NSA maneja, un informe del Servicio de Investigación del Congreso de Estados Unidos afirmaba lo siguiente: "Whereas NSA once predicted it was in danger of becoming proverbially deaf due to the spreading use of encrypted communications, it appears that NSA may now be at greater risk of being 'drowned' in information" (Seifert, 2007: 18).

ISBN-13: 978-84-16458-45-5 / D.L.: TF-162-2016 / DOI: 10.4185/cac103

derivadas tanto de los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la UE[9], como de los principios enunciados por el Tribunal de Justicia en la sentencia Digital Rights Ireland[10].

En realidad, en su recurso, el Sr. Schrems impugna la licitud del régimen de puerto seguro establecido por esa Decisión de la Comisión, que lleva a la autoridad nacional de control a desestimar sin investigar su reclamación. Ni se rebate formalmente la validez de la Directiva 95/46/CE ni la de la Decisión 2000/520/CE. Sin embargo, la cuestión a dilucidar reside en averiguar si, en virtud del artículo 25.6 de esa Directiva, la Comisaria estaba vinculada por la constatación realizada por la Comisión en su Decisión, según la cual Estados Unidos garantiza un nivel de protección adecuado, o bien si el artículo 8 de la Carta de los Derechos Fundamentales de la UE le autorizaba a separarse de esa constatación y, por tanto, debería haber investigado antes de rechazar la reclamación presentada por el Sr. Schrems.

Así las cosas, la alta instancia judicial irlandesa decidió suspender el procedimiento y plantear al Tribunal de Justicia la cuestión prejudicial. Lo que se quería conocer era si una Decisión por la que la Comisión constata que un tercer país garantiza un nivel de protección adecuado, impide a una autoridad de control de un Estado miembro examinar la solicitud de una persona relativa a la protección de sus derechos y libertades frente al tratamiento de los datos personales que le 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.

Para ello, el Tribunal de Justicia tenía que interpretar el artículo 25.6 de la Directiva 95/46/CE, a la luz de los artículos 7, 8 y 47 de la Carta. Con dicha interpretación se lograría saber si la Decisión podía impedir a una autoridad nacional de control investigar una denuncia en la que se alega que un país

[9] El derecho al respeto de la vida privada garantizado por el artículo 7 de la Carta y por los valores esenciales comunes a las tradiciones de los Estados miembros perdería su significación si se permitiera a los poderes públicos acceder a las comunicaciones electrónicas de manera aleatoria y generalizada, sin ninguna justificación objetiva fundada en razones de seguridad nacional o prevención de la delincuencia ligadas específicamente a los individuos afectados, sin que esas prácticas se rodeen de garantías adecuadas y comprobables.

[10] STJUE, 8 de abril de 2014, Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238.

ISBN-13: 978-84-16458-45-5 / D.L.: TF-162-2016 / DOI: 10.4185/cac103

tercero no garantiza un nivel de protección adecuado y, en su caso, suspender la transferencia de datos denunciada.

3. Las transmisiones de datos de carácter personal desde la UE a terceros países

El derecho a la protección de datos personales se ha desarrollado en el ordenamiento jurídico europeo tanto por vía normativa de las instituciones como a través de la jurisprudencia del Tribunal de Justicia[11], aunque su reconocimiento culmina con su inclusión en el artículo 8 de la Carta de los Derechos Fundamentales de la UE (Ruiz Miguel, 2003: 21). Este derecho está íntimamente ligado al que protege la vida privada, si bien en la actualidad tiene un tratamiento autónomo en la mayoría de los textos legales más modernos, como es el caso de la Carta de los Derechos Fundamentales de la UE (Kokott & Sobotta, 2013: 84).

Mientras en Estados Unidos existe una regulación dispersa de la protección de los datos personales en normas que se refieren a ámbitos específicos[12], en la UE se ha optado por una única norma marco que cubre todos los sectores que por cualquier razón compilen, almacenen y traten datos de este tipo, la Directiva 95/46/CE sobre protección de datos[13] que, a su vez, se ajusta a los

[11] Hay que señalar que la jurisprudencia no lo ha reconocido de forma autónoma desligado del derecho a la vida privada, aunque ha tenido algunas oportunidades, como por ejemplo, STJCE, 12 de noviembre de 1969, Eric Stauder v. Stadt ULM-SOZIALAMT, C-29/69, EU:C:1969:57; STJCE, 7 de noviembre de 1985, Stanley George Adams v. Comisión, C-145/83, EU:C:1985:448; STJCE, 21 de abril de 1994, Anna Maria Campogrande v. Comisión, C-22/93, EU:C:1994:164 (Piñar Mañas 2003: 66).

[12] Algunas de esas normas estadounidenses se incluyen en leyes que tienen que ver con el sector de la salud y que obligarían a la protección de los datos personales a las entidades de este ámbito (1996 Health Insurance Portability and Accountability Act). Igualmente ocurriría con las instituciones financieras (1999 Gramm-Leach-Bliley Act) o las relaciones laborales a través de varias leyes tanto estatales como federales.

[13] También tenemos la Directiva 2002/58/CE, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (DO L 201, 31.7.2002, p. 37), que incluye disposiciones sobre seguridad de las redes y los servicios, confidencialidad de las comunicaciones, acceso a la información almacenada en equipos terminales, tratamiento de los datos de tráfico y localización, identificación de la línea de origen, guías públicas de abonados y comunicaciones comerciales no solicitadas. Esa Directiva fue modificada por la Directiva 2006/24/CE, de 15 de marzo de 2006, relativa a la conservación de datos generados o tratados en relación con la prestación de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones (DO L 105, 13.4.2006, p. 54), que ha sido declarada invalida por la sentencia del TJUE, 8 de abril de 2014, Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238.

ISBN-13: 978-84-16458-45-5 / D.L.: TF-162-2016 / DOI: 10.4185/cac103

principios establecidos en el Convenio Nº 108 del Consejo de Europa (García Aguilar, 1999: 2)[14]. La transposición de esta Directiva en los ordenamientos jurídicos nacionales ha supuesto que los datos personales de los ciudadanos cuenten con una protección equivalente en toda la Unión (Téllez Aguilera, 2002: 35).

Para la transferencia de datos personales a terceros países, la Directiva 95/46/CE exige que esos Estados garanticen "un nivel adecuado de protección". El nivel adecuado se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencia 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 tercer país de que se trate, así como las normas profesionales y las medidas de seguridad en vigor (Kuner, 2013: 42).

Si se comprueba que un tercer país no garantiza un nivel adecuado de protección, los Estados miembros impedirán que se le transfieran datos personales. Como excepción se señala que podrá efectuarse dicha transferencia a un país tercero que no garantice un nivel de protección adecuado cuando sea necesaria o legalmente exigida para la salvaguardia de "un interés público importante"[15]. Por tanto, la transmisión es ilícita, a menos que se den unas condiciones de licitud, que son la existencia de un nivel de protección adecuado en el Estado de destino o, en defecto de tal nivel, una de las excepciones enumeradas en la propia Directiva.

Un elemento esencial de la protección de las personas frente al tratamiento de datos personales es la creación en todos los Estados miembros de autoridades de control independientes.

[14] Convenio Nº 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, que entró en vigor el 1 de octubre de 1985. Más tarde este Convenio fue completado por el Protocolo Adicional, de 8 de noviembre de 2001, al Convenio Nº 108 del Consejo de Europa, que entró en vigor el 1 de julio de 2007 y la Recommendation Nº R (87) 15 of the Committee of Ministers to Member States regulating the use of personal data in the police sector, 410th meeting, 17 September 1987.

[15] El Considerando 58 al aclarar el término sólo menciona las transferencias entre administraciones fiscales o aduaneras o los servicios de Seguridad Social.

ISBN-13: 978-84-16458-45-5 / D.L.: TF-162-2016 / DOI: 10.4185/cac103

El artículo 28.1 de la Directiva 95/46/CE impone a los Estados miembros la obligación de instituir una o varias autoridades públicas encargadas del control del cumplimiento de las normas de la Unión en materia de protección de las personas físicas respecto al tratamiento de sus datos personales.

La garantía de independencia de las autoridades nacionales de control pretende asegurar un examen eficaz y fiable del respeto de la normativa en materia de protección de los datos personales. Esa garantía se ha establecido para reforzar la protección de las personas y de los organismos afectados por las decisiones de dichas autoridades.

Las facultades de las que gozan las autoridades nacionales de control aparecen enumeradas de forma no exhaustiva en el artículo 28.3 de la Directiva 95/46/CE y entre ellas podemos destacar las facultades de investigación, como la de recabar toda la información necesaria para el cumplimiento de su misión de control, las habilidades efectivas de intervención, como la de prohibir provisional o definitivamente un tratamiento de datos, o la capacidad de comparecer en juicio.

Es verdad que conforme al apartado 1 de la misma disposición esas facultades de las autoridades nacionales de control abarcan los tratamientos de datos personales realizados en territorio de su Estado, de modo que no las pueden aplicar, con fundamento en el artículo 28, a los tratamientos de datos realizados en el territorio de un tercer país. Sin embargo, la operación de 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, en el sentido del artículo 2 de la Directiva 95/46/CE[16]. En efecto, este precepto define el tratamiento de datos personales como "cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales", y cita como ejemplo "la comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos".

[16] Véase a este respecto STJCE, 30 de mayo de 2006, Parlamento/Consejo y Comisión, C-317/04 y C-318/04, EU:C:2006:346, apartado 56.

ISBN-13: 978-84-16458-45-5 / D.L.: TF-162-2016 / DOI: 10.4185/cac103

Las transferencias de datos personales hacia terceros países solo podrán efectuarse si se respetan plenamente las disposiciones adoptadas por los Estados miembros en aplicación de la misma Directiva[17]. En ese sentido su capítulo IV, en el que figuran los artículos 25 y 26, establece un régimen dirigido a garantizar un control por los Estados miembros de las transferencias de datos personales hacia terceros países. Se trata de un régimen complementario del régimen general que instaura el capítulo II de la misma Directiva, en el que se incluyen las condiciones generales de licitud de los tratamientos de datos personales[18].

Como quiera que las autoridades nacionales de control, conforme al artículo 8.3 de la Carta y al artículo 28 de la Directiva 95/46/CE, están encargadas de supervisar el cumplimiento de las reglas de la Unión para la protección de las personas físicas frente al tratamiento de los datos personales, 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 exigencia establecidas por la Directiva 95/46/CE.

4. El régimen de puerto seguro

Los principios en los que se basa el régimen de puerto seguro fueron publicados por el Departamento de Comercio de Estados Unidos, junto a una serie de preguntas más frecuentes (FAQ) que los complementan e instruyen su aplicación en la práctica[19].

En el artículo 1.1 de esta Decisión, la Comisión manifestaba que esos principios, aplicados de conformidad con la orientación que proporcionan las FAQ, garantizan un nivel adecuado de protección de los datos personales transferidos desde la Unión a entidades establecidas en Estados Unidos.

[17] Considerando 60 de la Directiva.

[18] Véase, en este sentido, STJCE, 6 de noviembre de 2003, Lindqvist, C-101/01, EU:C:2003:596, apartado 63).

[19] Los principios figuran en el anexo I y las FAQ en el anexo II de la Decisión 2000/520/CE. También se pueden consultar todo lo relacionado con el programa de puerto seguro (principios, FAQ, lista de empresas adheridas, políticas de privacidad de dichas empresas, entidades que no han renovado, etc.) en la siguiente página: <http:export.gov/safeharbor/eu/eg_main_018476. asp> (última consulta 15 octubre 2015).

ISBN-13: 978-84-16458-45-5 / D.L.: TF-162-2016 / DOI: 10.4185/cac103

Cualquier compañía que quería adherirse al régimen de puerto seguro debía desarrollar una política de privacidad sujeta a los principios de notificación, elección, transferencia sucesiva, seguridad, integridad de los datos, acceso y ejecución. No se trataba de normas vinculantes, sino de una serie de directrices voluntarias que una organización puede certificar que sigue (Greer, 2011: 144).

Como la Directiva, los principios incluidos en el régimen de puerto seguro buscaban empoderar al sujeto, requiriendo se fuera informado sobre el fin para el que sus datos iban a ser usados, dándole la oportunidad de elegir si sus datos podían ser usados para finalidades distintas a las que en un principio justificaron su recogida, y permitiéndole el acceso a sus datos para corregirlos, enmendarlos o suprimirlos cuando fuera necesario.

Los principios también imponían obligaciones al responsable del tratamiento, como asegurarse de que los datos personales eran relevantes y fiables para el fin pretendido y que solo fueran transferidos a organizaciones consideradas "adecuadas". Además, los responsables del tratamiento debían tomar las precauciones necesarias para proteger los datos personales de posibles pérdidas o abusos y prever un mecanismo de recurso en manos de los particulares para resolver las controversias sobre privacidad y reclamar los posibles daños producidos[20].

El principio de ejecución obligaba a la compañía que quería adherirse al régimen de puerto seguro a establecer un mecanismo para certificar que cumplía con los Principios y este mecanismo podía ser una autocertificación o a través de una revisión externa.

Cuando una compañía desarrollaba una política de privacidad integral basada en los siete principios del régimen de puerto seguro debía hacerla accesible al público en general, por ejemplo, publicándola en su página web. De otra forma, los individuos cuyos datos personales eran recopilados y sometidos a

[20] El posible mecanismo de resolución de conflictos puede ser proporcionado a través de órganos autoregulados provenientes del sector privado, entidades legales o reglamentarias de supervisión o comprometiéndose a cooperar con las autoridades europeas de protección de datos. Un ejemplo de la primera opción lo constituye TRUSTe, una organización de solución de disputas que ya ha tomado decisiones en más de 4.000 reclamaciones presentadas por ciudadanos europeos frente a compañías estadounidenses acogidas al régimen de puerto seguro.

ISBN-13: 978-84-16458-45-5 / D.L.: TF-162-2016 / DOI: 10.4185/cac103

tratamiento no conocerían sus derechos y tampoco serían conscientes de las obligaciones a las que la compañía está sometida[21].

Resumiendo, cuando una compañía había promulgado reglas prácticas para el tratamiento de datos personales de acuerdo con los Principios, había incentivado el cumplimiento de las mismas a través de una política de privacidad públicamente accesible, había establecido un mecanismo independiente de resolución de conflictos que dará respuesta a las posibles reclamaciones y había implementado un sistema para verificar la futura conformidad con los Principios, entonces esa compañía estaba preparada para participar formalmente en el régimen de puerto seguro (Colonna, 2014: 206).

Lo cierto es que la adhesión de una entidad a los principios de puerto seguro se llevaba a cabo conforme a un sistema de autocertificación[22]. Esto significa que la compañía americana señalaba que suscribía los principios y que los cumplía realmente, dentro de su política de privacidad. A continuación notificaba al Departamento de Comercio de Estados Unidos su conformidad con esos principios. Anualmente cada compañía debía renovar su inscripción en dicho registro certificando que seguía cumplimiento con los requisitos de puerto seguro. Si una empresa salía de la lista, las reglas de protección garantizadas por el régimen de puerto seguro se seguirían aplicando a los datos que fueron obtenidos durante el periodo que se acogió a los principios asociados a tal régimen.

Como decimos el Departamento de Comercio estadounidense era el encargado de recibir y revisar todas las autocertificaciones de adhesión a los principios de puerto seguro y todas las comunicaciones anuales de renovación, manteniendo al día una lista con las empresas que habían presentado esta documentación.

Pero para el caso de declaraciones falsas de adhesión o incumplimiento de los principios de puerto seguro por parte de entidades participantes, la encargada de la investigación era la Comisión Federal de Comercio (*Federal Trade*

[21] Comunicación de la Comisión 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, de 27 de noviembre de 2013, COM (2013) 847.
[22] Artículo 1, apartados 2 y 3, de la Decisión 2000/520, en relación con la FAQ nº 6, anexo II.

ISBN-13: 978-84-16458-45-5 / D.L.: TF-162-2016 / DOI: 10.4185/cac103

Commission), que intervenía contra prácticas desleales y fraudulentas para los consumidores conforme a la *Federal Trade Commission Act* de 1914[23].

5. La decisión del caso Facebook

5.1. Implicaciones del fallo

En la sentencia del caso Facebook, el Tribunal de Justicia invalida la Decisión 2000/520/CE por la que la Comisión, apoyándose en el régimen de puerto seguro, declaraba que las normas americanas garantizaban un nivel adecuado de protección de los datos transferidos desde la Unión a compañías situadas en Estados Unidos.

Pero la sentencia no entra a valorar los principios de puerto seguro porque, a la hora de dictar esa Decisión, la Comisión no comprobó que Estados Unidos garantizara efectivamente un nivel de protección adecuado en razón de su legislación interna o sus compromisos internacionales. Por ello, el artículo 1 de dicha Decisión vulnera las exigencias establecidas en el artículo 25.6 de la Directiva 95/46/CE, entendido a la luz de la Carta y es inválido por dicha causa.

La sentencia también declara inválido en artículo 3 de la Decisión que establece la regulación específica de las facultades de las que disponen las autoridades nacionales de control ante la constatación realizada por la Comisión sobre el nivel de protección adecuado.

Según dicha disposición, las autoridades referidas, "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, […] podrán ejercer su facultad de suspender los flujos de datos hacia una entidad que haya autocertificado su adhesión a los principios", exigiendo para dicha intervención un umbral muy alto de condiciones. Aunque esta disposición no enerva las facultades de las autoridades nacionales de control para tomar medidas encaminadas a asegurar el cumplimiento de las disposiciones nacionales adoptadas en aplicación de la Directiva, excluye en cambio la posibilidad de que esas

[23] En el caso específico de la aplicación de los principios de puerto seguro a las compañías aéreas, el órgano competente es el Departamento de Transporte de Estados Unidos (Título 46, § 41712 US Code).

ISBN-13: 978-84-16458-45-5 / D.L.: TF-162-2016 / DOI: 10.4185/cac103

autoridades tomen medidas con objeto de asegurar el cumplimiento del artículo 25 de la Directiva.

Por ello, el artículo 3 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, en el supuesto de que una persona alegue, con ocasión de una solicitud basada en dicha disposición, factores que puedan afectar a la compatibilidad de una decisión de la Comisión, que haya constatado con fundamento en el artículo 25.6 de la Directiva que un tercer país garantiza un nivel adecuado de protección, con la preservación de la vida privada y de las libertades y derechos fundamentales de las personas. Y la Comisión no posee la competencia para restringir las facultades de las autoridades nacionales de control atribuidas por la Directiva. El Tribunal considera invalido el artículo porque todo lo dicho hasta el momento prueba que se adoptó excediendo los límites de la competencia que esta institución posee en base al artículo 25.6 de la Directiva.

El órgano judicial europeo remata su argumentación diciendo que toda vez que los artículos 1 y 3 de la Decisión 2000/520/CE son indisociables de los artículos 2 y 4 y de los anexos de ésta, su invalidez tiene el efecto de afectar a la validez de esa Decisión en su conjunto[24].

5.2. Precisión del papel de las autoridades nacionales de control

Conforme al artículo 25 de la Directiva 95/46/CE, la Comisión estaba facultada para constatar si un país tercero garantiza o no un nivel de protección adecuado.

La decisión así adoptada tiene por destinatarios los Estados miembros, que deberán aprobar las medidas necesarias para atenerse a ella. En virtud del artículo 288 TFUE, párrafo cuarto, esa decisión es obligatoria para todos los Estados miembros destinatarios y vincula por tanto a todos los órganos[25], en

[24] Apartado 105 de la sentencia.

[25] Véase, en este sentido, STJCE, 21 de mayo de 1987, Albako/BALM, C-249/85, EU:C:1987:245, apartado 17, y STUE, 13 de febrero de 2014, Mediaset, C-69/13, EU:C:2014:71, apartado 23.

ISBN-13: 978-84-16458-45-5 / D.L.: TF-162-2016 / DOI: 10.4185/cac103

cuanto tiene el efecto de autorizar transferencias de datos personales desde los Estados miembros al tercer país al que se refiere dicha decisión.

Así pues, mientras la decisión de la Comisión no haya sido declarada invalida por el Tribunal de Justicia, única instancia competente para dicha declaración, los Estados miembros y sus órganos, entre ellos las autoridades de control independientes, no pueden tomar 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. Y ello es así porque los actos de las instituciones de la Unión disfrutan en principio de presunción de legalidad y producen efectos jurídicos mientras no hayan sido revocados o anulados en virtud de un recurso de anulación o declarados inválidos a raíz de una cuestión prejudicial o de una excepción de ilegalidad[26].

No obstante, una decisión de la Comisión adoptada en virtud del artículo 25.6 de la Directiva 95/46/CE, como es el caso de la Decisión 2000/520/CE, 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 misma Directiva, 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 Directiva, como expuso el Abogado General en los puntos 61, 93 y 116 de sus conclusiones.

Concretamente, el artículo 28.4 de la Directiva 95/46/CE dispone que las autoridades nacionales de control entenderán de la solicitud que presente "cualquier persona […] en relación con la protección de los derechos y libertades respecto del tratamiento de datos personales" y no prevé ninguna excepción para el supuesto de que la Comisión haya adoptado una decisión en virtud del artículo 25.6 de la misma Directiva.

[26] STJCE, 5 de octubre de 2004, Comisión/Grecia, C-475/01, EU:C:2004:585, apartado 18 y la jurisprudencia ahí citada.

Así lo ponía de relieve la propia Comisión en su tercer informe de revisión del programa de puerto seguro realizada en 2013[27]. En casos específicos las autoridades nacionales de control están facultadas para suspender las transferencias de datos a una entidad que haya certificado su adhesión a los principios de puerto seguro conforme a lo dispuesto en la Decisión 2000/520/CE. Esos casos específicos son, entre otros, que existan grandes probabilidades de que se están vulnerando los principios o que la continuación de la transferencia podría crear un riesgo inminente de grave perjuicio a los afectados, situaciones aplicables al caso Facebook[28]. Independientemente de las facultades que les otorga esa Decisión, las autoridades nacionales de control están facultadas para intervenir, incluso en caso de transferencias internacionales, a fin de garantizar el cumplimiento de los principios generales en materia de protección de datos proclamados en la Directiva 95/46/CE.

El Tribunal de Justicia afirma que sería contrario al sistema establecido por la Directiva 95/46/CE y a la finalidad de sus artículos 25 y 28 que una decisión de la Comisión adoptada en virtud del artículo 25.6 de esa 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.

Por el contrario, el artículo 28 se aplica por su propia naturaleza a todo tratamiento de datos personales. Por tanto, incluso habiendo adoptado la Comisión una decisión al respecto, las autoridades nacionales de control, a las que una persona haya presentado una solicitud de protección de sus derechos y libertades frente al tratamiento de datos personales que la conciernen, deben poder apreciar con toda independencia si la transferencia de esos datos cumple las exigencia establecidas en la repetida Directiva.

[27] Comunicación de la Comisión al Parlamento Europeo y al Consejo, de 27 de noviembre de 2013, 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 final.
[28] Artículo 3.1 b) de la Decisión 2000/520/CE.

ISBN-13: 978-84-16458-45-5 / D.L.: TF-162-2016 / DOI: 10.4185/cac103

Si no fuera así, los ciudadanos europeos cuyos datos personales hayan sido o pudieran ser transferidos al tercer país considerado quedarían privados del derecho garantizado por el artículo 8, apartados 1 y 3, de la Carta de los Derechos Fundamentales de UE, esto es, su derecho a presentar a las autoridades nacionales de control una solicitud para la protección de sus derechos fundamentales[29].

Esto significa que la solicitud que presentó el Sr. Schrems, donde alegaba que Estados Unidos no garantizaba un nivel de protección adecuado, a pesar de la Decisión 2000/520/CE, debió entenderse como concerniente en sustancia a la compatibilidad de la Decisión con la protección de la vida privada y de las libertades y derechos fundamentales de las personas. Nos recuerda el Tribunal de Justicia que la Unión Europea 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"[30]. Por tanto, las decisiones de la Comisión adoptadas en virtud del artículo 25.6 de la Directiva 95/46/CE no pueden quedar excluidas de ese control.

5.3. Sobre la adecuación de la protección de los datos personales

La Directiva 95/46/CE, en su artículo 25.6, dispone que 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" (González Fuster, 2014: 168).

[29] Véase, por analogía, STJUE, 8 de abril de 2014, Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartado 68.

[30] Véanse, en este sentido, STJUE, 18 de julio de 2013, Comisión y otros /Kadi, C-584/10 P, C-593/10 P y C-595/10 P, EU:C:2013:518, aparatado 66; STJUE, 3 de octubre de 2013, Inuit Tapiriit Kanatami y otros/Parlamento y Consejo, C-583/11 P, EU:C:2013:625, apartado 91, y STJUE, 19 de diciembre de 2013, Telefónica/Comisión, C-274/12 P, EU:C:2013:852, apartado 56.

ISBN-13: 978-84-16458-45-5 / D.L.: TF-162-2016 / DOI: 10.4185/cac103

Pero la Directiva no contiene una definición del concepto de "nivel de protección adecuado". Es más, 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.

El Grupo de Trabajo sobre protección de datos, tomando en cuenta la Directiva y otros instrumentos internacionales sobre protección de datos[31], apuntó una serie de principios de contenido y de requisitos de procedimiento, cuyo cumplimiento pudiera considerarse la condición mínima para juzgar adecuada la protección[32]. Los principios relativos al contenido apuntan a la limitación de objetivos, la proporcionalidad y calidad de los datos, la transparencia, la seguridad, el acceso, rectificación y oposición y la restricción respecto a transferencias sucesivas a terceros países. En algunos casos será necesario ampliar la lista, mientras que en otros puede reducirse. En cuanto a los requisitos de procedimiento es importante que se ofrezca un nivel satisfactorio de cumplimiento de las normas, apoyo y asistencia a los interesados y vías de recurso para los perjudicados.

Sin duda, del artículo 25.6 de la Directiva 95/46/CE se desprende que la Unión pretende asegurar la continuidad de su elevado nivel de protección incluso en caso de transferencia de datos personales a un tercer país. Sin embargo, es verdad que el término "adecuado" no significa que un tercer país garantice idéntico nivel de protección al del Derecho de la Unión. Exigir el cumplimiento de un modelo análogo de garantías haría imposible los flujos de datos que nuestra sociedad de la información precisa.

[31] Especialmente el Convenio nº 108 del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de 1981 y las Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales de 1980. También se tienen en consideración las reglas de Asia-Pacific Economic Cooperation Privacy Framework, de Economic Community of West African States Supplementary Act on Personal Data Protection y de la Resolución de la Asamblea General de Naciones Unidas de 18 de diciembre de 2013 sobre privacidad en la era digital.

[32] Grupo de Protección de datos del Artículo 29, Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos en la UE, WP 12, 24 de julio de 1998.

ISBN-13: 978-84-16458-45-5 / D.L.: TF-162-2016 / DOI: 10.4185/cac103

Si no se requiere identidad, al menos debe entender la expresión "nivel de protección adecuado" en el sentido de que se exige un nivel de protección sustancialmente equivalente al garantizado por la Unión[33]. A falta de esta exigencia, la Unión vería frustrado su objetivo de continuar con un elevado nivel de protección incluso en caso de transferencia de datos personales a un tercer país. Además, el elevado nivel de protección garantizado por la Directiva 95/46/CE, entendida a la luz de la Carta de los Derechos Fundamentales de la UE, se podría eludir fácilmente con transferencias de datos personales desde la Unión a terceros países para su tratamiento en éstos.

Los medios de los que se sirve ese tercer país para garantizar un nivel de protección sustancialmente equivalente al de la Unión pueden ser diferentes a los aplicados para preservar el cumplimiento de las exigencias de la Directiva 95/46/CE, eso sí, deben ser eficaces para alcanzar el resultado en la práctica. Por ello, al valorar la garantía ofrecida por un tercer país la Comisión está obligada a apreciar el contenido de las reglas aplicables en ese país, derivadas de la legislación interna o de los compromisos internacionales, así como la práctica seguida para asegurar el cumplimiento de esas reglas, debiendo atender esa institución a todas las circunstancias relacionadas con una transferencia de datos personales a un tercer país.

De igual modo, dado que el nivel de protección garantizado por un tercer país puede evolucionar, incumbe a la Comisión, tras adoptar una decisión conforme al artículo 25.6 de la Directiva 95/46/CE, comprobar periódicamente si sigue siendo fundada en Derecho y de hecho la constatación sobre el nivel de protección adecuado garantizado por el tercer país en cuestión, máxime cuando hay indicios que generan una duda en ese sentido.

Pero, la Comisión no posee el monopolio para apreciar el carácter adecuado del nivel de protección garantizado por un tercer país. También las autoridades nacionales de control y los tribunales nacionales estarán compelidos a tener en

[33] Llamando la atención sobre la intrusión en la soberanía de los países terceros que esta exigencia supone, Bauchner explica del siguiente modo la adecuación que exige la normativa europea: "While adecuacy is not as strict as equivalency, it nevertheless demands a certain level of aquiescence to (EU) law by thrid-partu countries if they are to continue those relations with Member States" (Bauchner 2000: 691).

ISBN-13: 978-84-16458-45-5 / D.L.: TF-162-2016 / DOI: 10.4185/cac103

cuenta las circunstancias sobrevenidas después de la adopción de la decisión por parte de la Comisión.

En conclusión, la Comisión cuando adopta una decisión de conformidad con el artículo 25.6 de la Directiva 95/46/CE debe realizar un control estricto de las exigencias del artículo 25 de la misma Directiva, entendida a la luz de las exigencias de la Carta de los Derechos Fundamentales de la UE[34].

5.4. El desenlace fatal del programa de puerto seguro

Ya hemos comentado que un sistema de autocertificación no es por sí mismo contrario a lo dispuesto en el artículo 25.6 de la Directiva 95/46/CE, y que la fiabilidad de este sistema en relación con la exigencia de un nivel de protección adecuado descansa, en esencia, en el establecimiento de mecanismos eficaces de detección y 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 a la protección de los datos personales.

El sistema se aplica a las entidades privadas pero no a las autoridades públicas de Estados Unidos, cuyas posibles injerencias en los derechos fundamentales de las personas no encuentran límites específicos y definidos. Las exigencias de seguridad nacional, interés público y cumplimiento de la ley permiten dichas injerencias.

Estados Unidos y la UE, sobre todo la Comisión, deberían haber aclarado el ámbito de aplicación de dicha excepción, a fin de evitar cualquier interpretación o aplicación que anulase en esencia el derecho fundamental a la intimidad y la protección de datos. En todo caso, esa excepción nunca debería haberse utilizado en menoscabo de la protección garantizada por la Carta y el resto de la legislación europea en materia de protección de datos. Recordemos que, de acuerdo con el artículo 52.1 de la Carta, las injerencias en el derecho a la protección de datos de carácter personal son posibles siempre que, respetando el contenido esencial del derecho, se prevean en una norma, respondan a un

[34] Véase, por analogía, STJUE, 8 de abril de 2014, Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartados 47 y 48.

ISBN-13: 978-84-16458-45-5 / D.L.: TF-162-2016 / DOI: 10.4185/cac103

interés general y sean necesarias y proporcionadas, requisitos deben aplicarse de manera especialmente rigurosa (González Pascual, 2014: 951).

Pero la pregunta que procede hacerse es si realmente existen tales injerencias. Según se desprende de dos Comunicaciones elaboradas en 2013[35], la propia Comisión ha constatado que las autoridades estadounidenses podían acceder a los datos personales transferidos desde los Estados miembros y tratarlos de manera incompatible con las finalidades de esa transferencia, que va más allá de lo estrictamente necesario y proporcionado para la protección de la seguridad nacional. El Parlamento Europeo considera que el acceso a gran escala de las agencias de inteligencia de Estados Unidos a los datos personales de la UE procesados en virtud del principio de puerto seguro no cumple los criterios de exención en materia de seguridad nacional[36]. El hecho de que las agencias de inteligencia americanas hayan tenido acceso de forma generalizada a los datos personales de los ciudadanos europeos pone de relieve que la protección de los mismos no es la adecuada (Zalnieriute 2015: 101).

Las excepciones o las limitaciones al derecho a la protección de datos personales no deben exceder de lo estrictamente necesario[37]. Pues bien, 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 resultado a alcanzar 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

[35] Comunicación de la Comisión al Parlamento Europeo y al Consejo titulada «Restablecer la confianza en los flujos de datos entre la Unión Europea y los Estados Unidos de América» [COM (2013) 846 final] de 27 de noviembre de 2013, y Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la Unión y las empresas establecidas en la Unión [COM (2013) 847 final] de 27 de noviembre de 2013.

[36] Resolución del Parlamento Europeo, de 12 de marzo de 2014, sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU., los órganos de vigilancia de 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.

[37] Véase STJUE, 8 de abril de 2014, Digital Rights Ireland y otros, C- 293/12 y C-594/12, EU:C: 2014:238, apartado 52 y la jurisprudencia ahí citada).

ISBN-13: 978-84-16458-45-5 / D.L.: TF-162-2016 / DOI: 10.4185/cac103

injerencia que constituyen tanto el acceso a esos datos como su utilización posterior[38].

La normativa del país tercero debe ofrecer protección jurídica contra posibles arbitrariedades e indicar claramente el alcance de la discrecionalidad y de las potestades de las autoridades públicas.

5.5. Ausencia de garantías frente a los abusos

Del mismo modo, la Comisión consideraba que las personas afectadas no disponían de vías jurídicas administrativas o judiciales que les permitían acceder a los datos que les concernían y obtener, en su caso, su rectificación o supresión. Y una normativa que no prevé posibilidad alguna de que el justiciable posea acciones legales para acceder a sus datos personales o para obtener su rectificación o supresión vulnera el contenido esencial del derecho fundamental a la tutela judicial efectiva.

En lo que atañe al nivel de protección de las libertades y derechos fundamentales garantizado en la Unión, según reiterada jurisprudencia del Tribunal de Justicia, 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 riesgos de abuso y contra cualquier acceso o utilización ilícitos de los mismos. La necesidad de disponer de esas garantías es aún más importante cuando los datos personales se someten a un tratamiento automático y existe riesgo elevado de acceso ilícito a ellos (Breyer, 2005: 369)[39].

[38] Véase, en este sentido, 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 las 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), y la STJUE, 8 de abril de 2014, Digital Rights Ireland y otros, C- 293/12 y C-594/12, EU:C: 2014:238, apartados 57 a 61.

[39] Véase STJUE, 8 de abril de 2014, Digital Rights Ireland y otros, C- 293/12 y C-594/12, EU:C: 2014:238, apartado 54 y 55 y la jurisprudencia ahí citada).

ISBN-13: 978-84-16458-45-5 / D.L.: TF-162-2016 / DOI: 10.4185/cac103

El Tribunal de Justicia afirma con rotundidad 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"[40]. 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"[41].

Por todo ello, el nivel de protección de los datos personales ofrecido por Estados Unidos no se considera equivalente al garantizado en la UE.

6. Conclusiones

En un contexto de globalización creciente y comunicación mundial, las transferencias de datos no están limitadas geográficamente, lo que supone un desafío de primer orden a la hora de legislar desde cualquier parte del mundo, cuando no se dispone de un marco jurídico común.

Las transferencias de datos personales a terceros países son necesarias, pero ello no obsta para que las mismas ofrezcan un nivel adecuado de protección, ya que cuando esto no es así se interfiere en la vida privada de cada individuo.

Conjugar la diversidad de normativas con la defensa de los derechos fundamentales en la Unión es el reto al que se enfrentan tanto las instituciones europeas como los Estados miembros.

La Carta de los Derechos Fundamentales de la UE reconoce el derecho a la protección de datos de carácter personal de forma autónoma, aunque íntimamente ligado a la privacidad. Por su parte, la Directiva 95/46/CE tiene por objeto garantizar la protección de las libertades y de los derechos fundamentales de las personas físicas y, en particular, el derecho a la intimidad, en lo que respecta al tratamiento de los datos personales. Esta legislación permite los flujos de esos datos a terceros países, aunque les exige

[40] Apartado 94 de la sentencia, que a su vez se apoya en la STJUE, 8 de abril de 2014, Digital Rights Ireland y otros, C- 293/12 y C-594/12, EU:C: 2014:238, apartado 39.
[41] Apartado 95 de la sentencia.

ISBN-13: 978-84-16458-45-5 / D.L.: TF-162-2016 / DOI: 10.4185/cac103

acreditar un nivel de protección adecuado que, en definitiva, significa un nivel de protección sustancialmente equivalente al de la Unión.

Como las transmisiones de datos a empresas americanas son regulares es importante contar con mecanismos que permitan una constatación rápida y segura de la adecuación del nivel de protección. A esta exigencia respondía el régimen de puerto seguro configurado por el Departamento de Comercio de Estados Unidos y avalado por la Comisión en su Decisión 2000/520/CE. Las empresas que autocertificasen que cumplían con los principios de dicho régimen eran automáticamente consideradas como garantes de un nivel de protección adecuado de los datos transferidos desde la Unión.

Sin embargo, la noticia de los programas de vigilancia masiva por parte de las agencias estatales estadounidenses, que se han servido de los datos exportados a las sedes centrales de compañías como Facebook, Apple o Google, encendió todas las alarmas, dando lugar a reclamaciones como la que se encuentra en el origen de la sentencia de 6 de octubre de 2015.

La principal consecuencia práctica de esta sentencia es que la Decisión 2000/520/CE ya no sirve como marco legal para la transferencia de datos personales desde la UE a Estados Unidos, por lo que entrará en juego el resto del artículo 25 de la Directiva 95/46/CE. Después de 15 años haciendo descansar los flujos de ingentes cantidades de datos de carácter personal en el régimen de puerto seguro, las empresas estadounidenses ya no podrán autocertificar una protección adecuada de los datos personales acudiendo a dicho régimen. Ahora las compañías estadounidenses deberán cumplir con los parámetros europeos de protección, que son más estrictos en cuanto a la privacidad de los datos y su garantía. Si las empresas no observan esta legislación corren el riesgo de que la autoridad nacional de control prohíba provisional o definitivamente la transferencia y el tratamiento de esos datos e imponga las correspondientes sanciones económicas.

La primacía de las exigencias de seguridad nacional, interés público y cumplimiento de ley sobre los principios de puerto seguro ha permitido una injerencia de las agencias estatales estadounidenses en los derechos fundamentales de los ciudadanos europeos, violando su intimidad y la

ISBN-13: 978-84-16458-45-5 / D.L.: TF-162-2016 / DOI: 10.4185/cac103

protección de sus datos personales. Aunque el carácter de esta interferencia en teoría sea excepcional, lo cierto es que la legislación estadounidense no limita las posibles intromisiones en los derechos fundamentales de las personas por parte de los poderes públicos.

Según la Carta de los Derechos Fundamentales de la UE, las injerencias en el derecho a la protección de datos personales deben respetar el contenido esencial del derecho, estar previstas en una norma, responder a un interés general y ser necesarias y proporcionadas. Estos extremos no fueron comprobados por la Comisión cuando adoptó la Decisión sobre puerto seguro, ahora anulada, y las revelaciones de Edward Snowden han puesto en tela de juicio las garantías generales del ordenamiento jurídico estadounidense. Garantizar el flujo de datos desde la Unión requiere que la normativa del país tercero ofrezca protección jurídica contra posibles arbitrariedades e indique claramente el alcance de la discrecionalidad y de las potestades de las autoridades públicas.

Con la Decisión 2000/520/CE declarada inválida, tenemos que preguntarnos cómo se va a articular el constante flujo de datos personales desde la Unión a Estados Unidos. Mientras no se acuerde un nuevo marco de referencia, a las compañías afectadas no les queda otro remedio que asegurarse de cumplir con los requisitos que exige la normativa europea. El primer cauce para ello estribaría en recabar el consentimiento libre y explícito de cada usuario para la transmisión de sus datos, lo cual además de caro y lento resulta demasiado rígido en un mundo tan versátil y dinámico como el de las comunicaciones electrónicas.

Pero no es la única opción, existen otras dos vías que las compañías americanas pueden seguir para conseguir la transferencia de datos de carácter personal de los ciudadanos europeos: las cláusulas contractuales tipo y las reglas corporativas vinculantes. En ambos casos, tanto las autoridades de protección de datos europeas, como las autoridades nacionales de control poseen poderes para investigar a las compañías que hayan optado por estos métodos.

ISBN-13: 978-84-16458-45-5 / D.L.: TF-162-2016 / DOI: 10.4185/cac103

Aún y todo, si tomamos en consideración que las dudas suscitadas por el Sr. Schrems respecto a la Decisión 2000/520/CE surgieron del programa de vigilancia Prims, la misma desconfianza podría plantearse tarde o temprano respecto a las cláusulas contractuales tipo o a las reglas corporativas vinculantes, dado que quizás su regulación tampoco asegure un nivel de protección adecuado después de revelados esos acontecimientos.

Por otra parte, gracias a la sentencia las autoridades nacionales de control han visto reforzada su posición para actuar cuando reciban reclamaciones de ciudadanos en relación con las transferencias de datos a países fuera de la Unión. Que exista una decisión de la Comisión que certifique un nivel de protección adecuado de los datos de carácter personal, no obsta a que la autoridad nacional de control que recibe la queja investigue el fondo de la misma y, si las circunstancias así los justifican, suspenda en parte o en su totalidad los flujos de datos hacia el Estado tercero.

Sin embargo, existe la posibilidad de que el mismo tipo de transmisiones de datos en idénticas circunstancias se suspendan por parte de la autoridad nacional de algún o algunos Estados miembros, mientras sigan existiendo respecto a los demás. Evitar estas incongruencias dentro del territorio de la UE es la razón que lleva a la Comisión a adoptar decisiones, como la que se declaró inválida, a través de las cuales se establece la adecuación de la protección ofrecida por el país tercero. Por tanto, no resulta sorprendente que la Unión y Estados Unidos ya estén negociando un nuevo marco de referencia para las transferencias de datos personales que, sin duda, vendrá certificado por otra decisión de la Comisión. Deseamos que en esta ocasión la institución europea realice un examen exhaustivo de la legislación estadounidense y de los compromisos internacionales de dicho país, para asegurarse de que realmente ofrece una protección “adecuada” de los datos de carácter personal que sus compañías reciben desde la UE.

ISBN-13: 978-84-16458-45-5 / D.L.: TF-162-2016 / DOI: 10.4185/cac103

7. Referencias bibliográficas

J Bauchner (2000): "State Sovereignty and the Globalizing Effects of the Internet: A Case Study of the Privacy Debate", en *Brooklyn Journal of International Law*, 26, páginas 689 a 722.

P Breyer (2005): "Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR", en *European Law Journal*, 11-3, páginas 365 a 375.

I Brown (2015): "The feasibility of transatlantic privacy-protective standards for surveillance", en International Journal of Law and Information Technology, 23, páginas 23-40.

L Colonna (2014): "Article 4 of the EU Data Protection Directive and the irrelevance of the EU-US Safe Harbor Program?", en *International Data Privacy Law*, 4-3, páginas 203 a 221.

N García Aguilar (1999): "Origen y significado del Convenio 108 del Consejo de Europa sobre protección de las personas con respecto al tratamiento automatizado de datos de carácter personal", en *Revista Internauta de Práctica Jurídica*, 2, páginas 1 a 22.

G González Fuster (2014): *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Heidelberg: Springer International Publishing.

M González Pascual (2014): "El TJUE como garante de los derechos de la UE a la luz de la sentencia Digital Rights Ireland", en *Revista de Derecho Comunitario Europeo*, 49, páginas 943 a 971.

D Greer (2011): "Safe Harbor – A Framework That Works", en *International Data Privacy Law*, 1-3, páginas 143 a 148.

J Kokott & C Julianne (2013): "The Distinction between privacy and data protection in the jurisprudence of the CJEU and the ECHR", en *International Data Privacy Law*, 3-4, páginas 83-95.

C Kuner (2013): *Transborder Data Flows and Data Privacy Law*, Oxford: Oxford University Press.

JL Piñar Mañas (2003): "El derecho a la protección de datos de carácter personal en la jurisprudencia del Tribunal de Justicia de las Comunidades Europeas", en *Cuadernos de Derecho Público*, 19-20, páginas 66 a 68.

C Ruiz Miguel (2003): "El derecho a la protección de datos personales en la Carta de Derechos Fundamentales de la Unión Europea: análisis crítico", en *Revista de Derecho Comunitario Europeo*, 14, páginas 7 a 43.

J Seifert (2007): *Data Mining and Homeland Security: An Overview*, Congressional Research Service report RL31798, Washington: Library of Congress.

A Téllez Aguilera (2002): *La protección de datos en la Unión europea. Divergencias normativas y anhelos unificadores*, Madrid: Edisofer.

M Zalnieriute (2015): "An international constitutional moment for data privacy in the times of mass-surveillance", en *International Journal of Law and Information Technology*, 23, páginas 99-133.

ISBN-13: 978-84-16458-45-5 / D.L.: TF-162-2016 / DOI: 10.4185/cac103