LA DECLARACIÓN DE INVALIDEZ DEL ACUERDO DE PUERTO SEGURO ENTRE LA UE Y LOS EEUU POR EL TJUE (C-362/14)

MARÍA ÁLVAREZ CARO

Abogada en la Asociación Española de la Economía Digital y colegiada del ICAM
Doctorando. MBA y Master en Protección de Datos, Transparencia y Acceso a la Información

MIGUEL RECIO GAYO

Abogado colegiado en el ICAM. Doctorando. Master en Protección de Datos, Transparencia y Acceso a la Información y Master en Derecho de la Propiedad Intelectual

Revista Española de Derecho Europeo 57
Enero – Marzo 2016
Págs. 107 – 136

SUMARIO: I. INTRODUCCIÓN Y ANTECEDENTES. *1. Consideraciones generales. 2. Resumen de los hechos. 3. Litigio y cuestiones prejudiciales.* II. EL NIVEL EUROPEO DE PROTECCIÓN DE DATOS PERSONALES. *1. La Carta de los Derechos Fundamentales de la Unión Europea. 2. La interpretación del Derecho de la UE conforme a la Carta de Derechos Fundamentales de la UE. 3. Límites a las injerencias a los derechos y las libertades fundamentales.* III. ALCANCE DE LAS FACULTADES DE LAS AUTORIDADES DE PROTECCIÓN DE DATOS. *1. Figura y funciones de las Autoridades de protección de datos conforme al artículo 28 de la Directiva 95/46/CE. 2. El papel de las Autoridades de protección de datos en el funcionamiento del Acuerdo de Puerto Seguro. 3. Delimitación y coordinación del ejercicio de las facultades de la Comisión Europea y las Autoridades de protección de datos.* IV. LA DECISIÓN 2000/520/CE SOBRE EL ACUERDO DE PUERTO SEGURO. *1. Análisis del TJUE sobre la validez de la Decisión 2000/520/CE. 2. Invalidez y consecuencias.* V. CONCLUSIONES.

RESUMEN: El pasado 6 de octubre de 2015, el TJUE dictó una sentencia que invalidó la Decisión 2000/520/CE de la Comisión Europea que declaraba el nivel adecuado en protección de datos del Puerto Seguro (Safe Harbour) entre EEUU y la UE conforme a la Directiva 95/46/CE de protección de datos. El fallo estima que una Decisión de la Comisión sobre el nivel adecuado de un tercer país no puede dejar sin efecto o limitar las facultades de las Autoridades Nacionales de Protección de Datos (APDs) de acuerdo con la Carta de Derechos Fundamentales de la UE y la citada Directiva. Asimismo, estima que la Decisión es inválida al preverse una excepción al régimen del acuerdo por motivos de seguridad nacional que supone un acceso sin límites y desproporcionado a los datos personales. Sin duda, este fallo abre un período de incertidumbre, en tanto no se apruebe un nuevo Puerto Seguro o se concreten soluciones sobre cómo realizar a partir de ahora las transferencias a EE.UU, algo que deberán aclarar la Comisión Europea y las APDs.

PALABRAS CLAVE: Protección de datos, Puerto Seguro, Directiva 95/46/CE, Carta de los Derechos Fundamentales de la Unión Europea, transferencias internacionales de datos a EEUU, nivel adecuado, autoridades de protección de datos, Comisión Europea.

ABSTRACT: On 6 October 2015, the European Court of Justice issued a ruling invalidating the Decision 2000/520/EC of the European Commission that declared the adequate level of data protection of the Safe Harbor (Safe Harbour) between the United States and the EU in accordance with Directive 95/46/EC for the protection of personal data. The ruling finds that a Decision of the Commission declaring the adequate level of a third country cannot nullify or limit the powers of the national data protection authorities (DPAs) in accordance with the Charter of Fundamental Rights of the EU and the mentioned Directive. It also estimates that the Decision is invalid for an exception to the rule of the agreement on the grounds of national security that supposes a disproportionate access and without limits to the data. Undoubtedly this ruling opens a period of uncertainty, until a new Safe Harbour is approved or any solutions given on how data transfers to the USA should be from now on, something that the European Commission and DPAs should clarify.

KEYWORDS: Data protection, Safe Harbour, Directive 95/46/EC, Charter of Fundamental Rights of the European Union, international data transfers to the USA, Data Protection Authorities, European Commission.

Fecha de envío del original: 21 de diciembre de 2015.
Fecha de aceptación: 15 de enero de 2016.

I. INTRODUCCIÓN Y ANTECEDENTES

1. CONSIDERACIONES GENERALES

La STJ, de 6.10.15, as. Schrems (C-362/14), resuelve, de manera conjunta, dos cuestiones prejudiciales planteadas por la *High Court* de Irlanda, al hilo de un caso que enfrenta a un ciudadano austríaco con la Autoridad de Protección de Datos (*Data Protection Commissioner*) irlandesa, relativa a la transferencia de datos de carácter personal a un tercer país fuera de la UE, en concreto por una red social, Facebook, en el caso de los datos personales de usuarios europeos desde Irlanda a los Estados Unidos (EEUU) utilizando el mecanismo del Acuerdo de Puerto Seguro (*Safe Harbour*). El fallo invalida la Decisión de la Comisión Europea que declaró que el Puerto Seguro con los EEUU garantizaba un nivel de protección de datos adecuado de los datos personales transferidos, lo que, sin lugar a dudas plantea una situación de inseguridad jurídica e incertidumbre[1] hasta que

1. El resultado de *Safe Harbour* puede ser descrito como un compromiso constructivo. Al respecto: Busch, A.: «From Safe Harbour to the rough sea? Privacy disputes across the Atlantic», *SCRIPT-Ed, A Journal of Law, Technology and Society*, vol. 3, nº 4, Junio 2006. En

las autoridades de protección de datos de la UE[2] ofrezcan unas directrices para que, los responsables y encargados del tratamiento de datos de carácter personal sepan claramente a qué atenerse, o bien hasta que EEUU y la UE avancen con el proceso de negociación de un nuevo acuerdo *Safe Harbour* o Puerto Seguro. Desde que en noviembre de 2013 la Comisión Europea (CE) publicó una Comunicación[3] sobre el funcionamiento del acuerdo en la que se detectaban deficiencias, dichos territorios negocian la renovación del mismo. El sistema *Safe Harbour* ha sido reconocido además como ventajoso durante todos estos quince años. «El sistema de Principios de Puerto Seguro, aunque ha sido criticado en algunas ocasiones, presenta ventajas, teniendo en cuenta que: constituye un marco normativo uniforme, permanente, estable y definitivo para la protección del derecho a la intimidad y para la transferencia internacional de datos de carácter personal entre la UE y los EEUU»[4].

La sentencia del TJUE, que valida las conclusiones del abogado general Y. Bot de poco más de una semana[5] antes de publicarse la sentencia, considera que las Autoridades de protección de datos pueden analizar –en su caso, pueden acudir a los tribunales nacionales para que éstos planteen una cuestión prejudicial sobre la validez de una Decisión de la CE que declara que un Estado cumple con las exigencias de la normativa europea de protección de datos–, si una transferencia de datos personales a un tercer Estado fuera de la UE cumple con las exigencias de la normativa europea, con independencia de que exista una Decisión de la Comisión Europea que declare que dicho país cumple con los requisitos de la normativa de la UE. En esta relevante y transcendental sentencia, por sus implicaciones en la práctica, se analizan las funciones y obligaciones de las Autoridades nacionales de protección de datos, la delimitación de funciones y la coordinación entre la Comisión Europea y dichas autoridades en la salvaguarda del derecho fundamental a la protección de datos de carácter personal de los ciudadanos, así como el propio régimen de Puerto Seguro del año 2000 para las transferencias internacionales de datos entre la UE y EEUU.

---

la misma línea, y resaltando la eficacia del régimen de Safe Harbour, tanto desde el punto de vista teórico como desde el práctico: Ortega Jiménez, A., «Algunas claves en las relaciones entre los EEUU y la UE sobre transferencias de datos de carácter personal», *Revista TELOS (Cuadernos de Comunicación e Innovación)*, mayo 2014, p. 1.

2. Las autoridades de protección de datos de la UE, junto con el Supervisor Europeo de Protección de Datos y la Comisión Europea conforman el órgano denominado Grupo de Trabajo del Artículo 29. Emiten dictámenes, opiniones y *guidelines* con alto valor doctrinal que normalmente son citadas por los tribunales de los Estados Miembros. Sus documentos, aunque sin rango de ley, tienen un elevado valor doctrinal.
3. Comunicación de la Comisión Europea al Parlamento Europeo y al Consejo de la UE sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos y de las empresas establecidas en la UE, de 27 de noviembre de 2013.
4. Ortega Jiménez, A.: «Algunas claves en las relaciones entre los EEUU y la UE sobre transferencias de datos de carácter personal», *Revista TELOS Cuadernos de Comunicación e Innovación*, Fundación Telefónica, febrero-mayo 2014, p. 1 a 7.
5. Conclusiones del Abogado General, Y. Bot, as. *Schrems*, (C-362/14), presentadas el 23.09.2015.

El TJUE invalida la Decisión 520/2000/CE de Puerto Seguro[6], al considerar que, a través de este tipo de Decisión, la Comisión Europea no puede dejar sin efecto ni limitar las facultades de las que disponen las autoridades de control nacionales con base en la Directiva 95/46/CE [7] y la Carta de Derechos Fundamentales de la UE (CDFUE)[8]. Asimismo, el TJUE insiste en que es la Comisión Europea quién está obligada a comprobar si EEUU garantiza un nivel adecuado de protección en función de su legislación interna o de sus compromisos internacionales, equivalente al existente en la UE en virtud de la Directiva 95/46/CE. Por otra parte, considera que en EEUU, las exigencias para la seguridad nacional, el interés público y el cumplimiento de la ley, prevalecen sobre el régimen de Puerto Seguro, de tal modo que las empresas adheridas al mismo están obligadas a dejar de aplicar, en EEUU, sin limitación, las reglas de protección previstas por ese régimen cuando entren en conflicto con las exigencias para la seguridad nacional.

Por ello, el TJUE observa que, puesto que existe una normativa que permite a las autoridades públicas estadounidenses acceder de forma generalizada, sin limitaciones ni excepciones, al contenido de comunicaciones electrónicas, se está lesionando por parte de las autoridades públicas americanas el derecho fundamental a la protección de datos de carácter personal, así como por las entidades que tratan datos en EEUU, estén o no adheridas a los principios de Puerto Seguro. Por ello, declara la invalidez de la Decisión 2000/520/CE y, como consecuencia, tanto empresas como la propia Administración esperan en este momento que tanto la propia Comisión Europea como las Autoridades de protección de datos de la UE agrupadas en el Grupo de Trabajo del Artículo 29 (WP 29 en adelante) arrojen, de manera conjunta y sin divergencias en el seno del mercado único digital europeo, algo de luz con respecto a las opciones o alternativas para las necesarias[9] transferencias internacionales de datos, tras la invalidez del *Safe Harbour*. En cierto modo, los pronunciamientos de esta sentencia están ligados a los que ya efectuó el WP

6. Decisión 520/2000/CE, de la Comisión, de 26.07.00, en la que se reconoce que los principios de puerto seguro para la protección de la vida privada y las preguntas más frecuentes publicadas por el Departamento de Comercio de EEUU ofrecen un nivel de protección adecuado a fines de la transferencia de datos personales desde la UE.

7. Directiva 95/46/CE, del Parlamento Europeo y del Consejo, de 24.10.1995, 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 (*DOUE*, nº L 281, de 23.11.1995).

8. Carta de los Derechos Fundamentales de la Unión Europea (*DOUE*, C 364/1, de 18.12.2000).

9. Las transferencias internacionales de datos han tenido una importancia creciente en términos económicos, políticos y sociales en los últimos años, desde la adopción en 1980 de las Guidelines de la OCDE para la protección de la privacidad y las transferencias internacionales de datos personales: Kuner, C., «Regulation of Transborder Data Flows under Data Protection and Privacy Law: past, present and future», *TILT Law & Technology*, *Working Paper* nº 016/2010, octubre 2010, p. 5.

29 en 2012[10] sobre los servicios de nube, así como en el caso específico del *Safe Harbour*, desde 1999 y en varias ocasiones[11].

La sentencia recoge asimismo que, en el punto 3.2 de la Comunicación (2013) 846 final[12], la Comisión señaló la existencia de diversas deficiencias en la aplicación de la Decisión 2000/520/CE y que la Directiva 95/46/CE debe ser necesariamente interpretada a la luz de los derechos fundamentales protegidos por la Carta de Derechos Fundamentales de la Unión Europea (UE), según destaca asimismo diversa jurisprudencia comunitaria[13].

2. RESUMEN DE LOS HECHOS

El 25 de junio de 2013 un ciudadano austríaco, el señor Schrems, usuario de la red social Facebook, presentó ante la Autoridad de Protección de Datos irlandesa una reclamación en la que le solicitaba que impidiera a Facebook Ireland, subsidiaria de la tecnológica americana, transferir sus datos personales a Estados Unidos, al

10. En el WP 196, de 1 de julio de 2012, el WP 29 manifestó que: «En ausencia de un sistema más robusto que vele por el cumplimiento de los principios de protección de datos en el entorno de la nube, obtener sólo la autocertificación de Puerto Seguro puede resultar insuficiente. […]. Las empresas en el ámbito de la UE que exporten datos no deberían de confiar exclusivamente en la declaración del importador de datos afirmando que posee la certificación de Puerto Seguro. Por el contrario, la empresa que exporte datos debería obtener pruebas de que las autocertificaciones de Puerto Seguro existen realmente y deberían solicitar pruebas que demostraran que se cumplen los principios relacionados con dichas autocertificaciones. Esto resulta especialmente importante en lo que respecta a la información proporcionada a los sujetos de datos a quienes afecta el procesamiento de datos».
11. En el WP 32, de 16 de mayo de 2000, el WP 29 afirmó, rotundamente, que «lamenta que los principios de Puerto Seguro se vean debilitados, por un lado, por una serie de excepciones introducidas por las preguntas más frecuentes y, por otro, por el apartado 5 de los principios (la adhesión a estos principios puede limitarse por disposición legal o reglamentaria, o jurisprudencia que originen conflictos de obligaciones o autorizaciones explícitas)». Y también señaló que «El Grupo de trabajo considera que el recurso a excepciones deberá controlarse cuidadosamente y que debería buscarse la cooperación con las autoridades estadounidenses para garantizar que las excepciones no se utilicen de forma que debiliten la protección que proporcionan los principios. En particular, el Grupo de trabajo opina que en un sistema adecuado de protección de datos el derecho de acceso no puede limitarse o denegarse de forma incompatible con la Directiva». En 1999 el WP 29 ya había emitido el WP 27, de 3 de diciembre de 1999 en el que manifestó que «El Grupo de trabajo reitera su preocupación por el hecho de que la adhesión a los principios pueda estar limitada por cualquier "disposición legal o reglamentaria, o jurisprudencia" [letra b) del párrafo 5 de los principios] sin más calificación».
12. Comunicación de la Comisión al Parlamento Europeo y al Consejo, Restablecer la confianza en los flujos de datos entre la UE y EEUU, COM (2013) 846 final, Bruselas, 27.11.2013.
13. STJ, de 20.5.2003, as. Österreichischner Rundfunk y otros (C-465/00, C-138/01 y C-139/01) –apartado 68–; STJ, de 13.5.2004, as. Google Spain y Google Inc (C-131/12) –apartado 68– y STJ, de 11.12.2014, as. Reynes (C-212/13), –apartado 29–.

considerar que dicho país, dadas las revelaciones de Edward Snowden[14] relativas a las injerencias de vigilancia de las autoridades públicas americanas[15], no satisfacía las exigencias para garantizar el cumplimiento de la normativa europea de protección de datos y, por tanto, no era un país con un nivel adecuado de protección según la Directiva 95/46/CE. Al parecer, según las afirmaciones del señor Schrems, Facebook Ireland transfiere total o parcialmente los datos personales de sus usuarios a Estados Unidos donde dicha plataforma tecnológica tiene su sede central[16].

Con carácter general, de acuerdo con la Directiva 95/46/CE no está permitido transferir datos personales desde la UE a terceros países situados fuera del Espacio Económico Europeo (EEE), salvo que las normas de protección de datos del Estado en cuestión al que se envían los datos hayan sido declaradas adecuadas por la Comisión Europea[17]

14. Ver el documento titulado *Five Myths regarding privacy and Law enforcement access to personal information in the European Union and the United States*, disponible en la dirección de Internet *http://photos.state.gov/libraries/useu/231771/PDFs/Five%20Myths%20Regarding%20Privacy%20and%20Law%20Enforcement_October%209_2012_pdf.pdf*.

15. Wright y Stupak resaltan que «Some EU officials, alarmed by reports of the NSA´s access to Internet companies, say Safe Harbor gives US companies a way to evade the EU´s more stringent privacy regime». Lo que puede traducirse como «Algunos oficiales de la UE, alarmados por los informes de la NSA sobre el acceso a las compañías de Internet, señalan que el Puerto Seguro ofrece a las compañías Americanas un camino para evitar el régimen más restrictivo de la UE sobre privacidad». Wright, D. y Stupak, R. J., *Surveillance in Europe*, Routledge, Estados Unidos de América, 2015, p. 16.

16. Al respecto, Colonna explica que «While these transfers are prima facie authorized pursuant to the EU-US Safe Harbor Agreement, Europe-versus-Facebook contends that, based on the revelation from Edward Snowden that Facebook provided the US government direct access to all personal data of its users to use in a massive electronic surveillance program entitled PRISM, there is no possibility that Facebook can demonstrate its actual compliance with the principles set forth in the program». Pudiendo traducirse al español como «Mientras que estas transferencias están, prima facie, autorizadas según el Acuerdo de Puerto UE-EE.UU, Europe-versus-Facebook sostiene que, con base en la revelación de Edward Snowden de que Facebook proporciona al gobierno Americano acceso directo a todos los datos personales de sus usuarios para que sean utilizados en un programa de vigilancia masiva electrónica denominado PRISM, no hay posibilidad de que Facebook pueda demostrar su cumplimiento actual con los principios establecidos en este programa». Colonna, L., «Europe Versus Facebook: An Imbroglio of EU Data Protection Issues», en *Data Protection on the Move*, Springer, 2016, p. 31.

17. Las once Decisiones adoptadas por la Comisión Europea en cuanto al nivel adecuado de terceros países, presentándolas en un orden alfabético por país, son las siguientes: (1) Decisión 2010/625/UE, de 19 de octubre de 2010, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la adecuada protección de los datos personales en Andorra; (2) Decisión 2003/490/CE de la Comisión, de 30 de junio de 2003, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina; (3) Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección de los datos personales conferida por la ley canadiense *Personal Information and Electronic Documents Act*;

o concurra alguna de las excepciones previstas en el apartado 1 del artículo 26 de la Directiva[18].

Por su parte, el Comisario Irlandés desestimó, por infundada, dicha solicitud, y consideró que no estaba obligado a investigar sobre los hechos denunciados sobre la base de la existencia de la Decisión 520/2000/CE de Puerto Seguro, por la que se

(4) Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003, relativa al carácter adecuado de la protección de los datos personales en Guernsey; (5) Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada dada en la Ley de las Islas Feroe sobre el tratamiento de datos personales; (6) Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004, relativa al carácter adecuado de la protección de los datos personales en la Isla de Man; (7) Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por el Estado de Israel en lo que respecta al tratamiento automatizado de los datos personales; (8) Decisión 2008/393/CE de la Comisión, de 8 de mayo de 2008, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales en Jersey; (9) Decisión de Ejecución 2013/65/UE de la Comisión, de 19 de diciembre de 2012, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por Nueva Zelanda; (10) Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa al nivel de protección adecuado de los datos personales en Suiza, y (11) Decisión de Ejecución 2012/484/UE de la Comisión, de 21 de agosto de 2012, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por la República Oriental del Uruguay en lo que respecta al tratamiento automatizado de datos personales.

18. El artículo 26, apartado 1, prevé las siguientes excepciones a la regla general de prohibición de transferencias internacionales a terceros países sin nivel adecuado: «1. No obstante lo dispuesto en el artículo 25 y salvo disposición contraria del Derecho nacional que regule los casos particulares, los Estados miembros dispondrán que pueda efectuarse una transferencia de datos personales a un país tercero que no garantice un nivel de protección adecuado con arreglo a lo establecido en el apartado 2 del artículo 25, siempre y cuando:
    a) el interesado haya dado su consentimiento inequívocamente a la transferencia prevista, o
    b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado, o
    c) la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero, o
    d) La transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial, o
    e) la transferencia sea necesaria para la salvaguardia del interés vital del interesado, o
    f) la transferencia tenga lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta».

reconoce que el *Safe Harbour* con EEUU garantiza un nivel de protección adecuado según los estándares europeos. El Comisario argumentó que cualquier cuestión relativa a las transferencias de datos de la UE a EEUU debía resolverse conforme a dicha Decisión del año 2000.

El reclamante, ante la respuesta recibida por parte de la Autoridad de Protección de Datos irlandesa, interpuso un recurso ante la *High Court* de Irlanda impugnando la licitud del régimen de Puerto Seguro, que apreció que un asunto de estas características debe resolverse a la luz del Derecho de la UE y que, por tanto, la legalidad de la Decisión discutida en el asunto principal, debe resolverse a la luz de los artículos 7 y 8 de la Carta de Derechos Fundamentales de la UE[19] y los principios enunciados por la jurisprudencia del TJUE, como en la sentencia Digital Rights Ireland[20], entre otros pronunciamientos.

3. LITIGIO Y CUESTIONES PREJUDICIALES

La sentencia tiene su origen en las cuestiones prejudiciales planteadas por la *High Court* de Irlanda al órgano jurisdiccional encargado de interpretar el Derecho comunitario, en concreto por las dudas interpretativas en relación con los artículos 7, 8 y 47 de la Carta de Derechos Fundamentales de la UE[21], de los artículos 25, apartado 6, y 28 de la Directiva 95/46/CE, así como en sustancia la validez de la Decisión 520/2000/CE de Puerto Seguro.

El caso, como ya se ha indicado, se plantea en el marco de un litigio entre el ciudadano austríaco Maximilian Schrems y *Data Protection Commission* (Autoridad de Protección de Datos) irlandesa. El reclamante interpone un recurso ante la *High Court* y ésta, ante las dudas interpretativas de Derecho comunitario, decide suspender el procedimiento y plantea al TJUE dos cuestiones prejudiciales:

1. En el marco de la resolución de una reclamación presentada ante el comisario, en la que se afirma que se están transmitiendo datos personales a un tercer país (en el caso de autos, Estados Unidos) cuya legisla-

19. El artículo 7 de la CDFUE dice así: «Respeto de la vida privada y familiar. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones». Por su parte, el artículo 8 CDFUE, relativo al derecho fundamental a la protección de datos, es como sigue: «Protección de datos de carácter personal. 1. Toda persona tiene derecho a la protección de los datos de carácter personal que la conciernen».

20. Ver la STJ, de 8.4.2014, as. C-293/12, por la que se declara inválida la Directiva de conservación de datos de 2006.

21. En el Título VI de la CDFUE, el artículo 47 señala: «Derecho a la tutela judicial efectiva y a un juez imparcial. Toda persona cuyos derechos y libertades garantizados por el Derecho a la Unión hayan sido violados tiene derecho a la tutela judicial efectiva respetando las condiciones establecidas en el presente artículo. Toda persona tiene derecho a que su causa sea oída equitativa y públicamente y dentro de un plazo razonable por un juez independiente e imparcial, establecido previamente por la ley. Toda persona podrá hacerse aconsejar, defender y representar. Se prestará asistencia jurídica gratuita a quienes no dispongan de recursos suficientes siempre y cuando dicha asistencia sea necesaria para garantizar la efectividad del acceso a la justicia».

ción y práctica no prevén una protección adecuada de la persona sobre la que versan los datos, ¿está vinculado dicho comisario en términos absolutos por la declaración comunitaria en sentido contrario contenida en la Decisión 2000/520/CE, habida cuenta de los artículos 7, 8, y 47 de la Carta y no obstante lo dispuesto en el artículo 25, apartado 6, de la Directiva 95/46/CE[22].

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

Las preguntas formuladas van dirigidas, por tanto, a que el TJUE aclare si los tribunales y autoridades de los Estados miembros están vinculados de forma absoluta por una Decisión de la Comisión Europea vigente que declare que determinado país, aunque en este caso se trata del Acuerdo de Puerto Seguro con los EEUU, cumple con las exigencias de la normativa de la UE en protección de datos[23], de modo que no puedan ni deban investigar o analizar si pese a la existencia de dicha Decisión no se dan las garantías necesarias. Se pregunta, por tanto, al TJUE si el artículo 25 apartado 6 de la Directiva 95/46/CE, interpretado de acuerdo con los artículos 7 y 8 de la CDFUE, permite dicha investigación por parte de las Autoridades de protección de datos y tribunales de los Estados miembros.

---

22. Artículo 25, apartado 6 de la Directiva 95/46/CE: «La Comisión podrá hacer constar, de conformidad con lo 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. Los Estados Miembros adoptarán las medidas necesarias para ajustarse a la decisión de la Comisión».

23. Al respecto, cabe considerar que Thompson y Wagonne explican que «In negotiating the substance of the US/EU Safe Harbor Principles, the US sought to advance certain policy goals. After examining the EU Privacy Directive and recognizing its potential impact on trans-Atlantic trade, Commerce and the FTC began to explore how to address the EU's data protection concerns while at the same time, respecting the sectoral approach of US data protection laws». Pudiendo traducirse como «En la negociación del fondo de los Principios del Puerto Seguro EEUU/UE, los EEUU trataron de avanzar ciertos objetivos de política pública. Después de examinar la Directiva de privacidad de la UE e identificar su impacto potencial en el comercio transatlántico, el Departamento de Comercio y de la Comisión Federal de Comercio comenzaron a explorar la forma de abordar las preocupaciones sobre protección de datos de la UE y, al mismo tiempo, respetar el enfoque sectorial de las leyes de protección de datos de Estados Unidos». Thompson M. W. y Van Wagonen Magee, P., «US/EU Safe Harbor Agreement: What It Is and What It Says About the Future of Cross Border Data Protection», *Privacy Regulation*, Spring 2003. p. 5. Disponible, en inglés, en *https://www.ftc.gov/system/files/documents/public_statements/418691/thompsonsafeharbor.pdf*.

Por su parte, la *High Court* irlandesa apreció que la vigilancia electrónica y la interceptación de los datos personales transferidos de la UE a EEUU servían a finalidades necesarias para el interés público, a la vez que reconocía expresamente que por parte de la Agencia de Seguridad Nacional de los EEUU (*National Security Agency*, NSA) y otros organismos federales, es decir, otras autoridades de vigilancia con acceso a datos personales, se habían cometido «importantes excesos». El alto tribunal irlandés recuerda asimismo que toda injerencia en el derecho a la vida privada requiere que se respete el principio de proporcionalidad y se ajuste a las exigencias previstas por la ley, siendo el acceso y vigilancia masiva manifiestamente contrario al principio de proporcionalidad. La *High Court* tiene asimismo claro que este asunto debe resolverse a la luz del Derecho de la Unión Europea, aunque para el propio tribunal irlandés la Decisión 2000/520/CE no se ajusta a los artículos 7 y 8 de la Carta y a los principios enunciados en la jurisprudencia comunitaria.

Cabe recordar que, desde un punto de vista formal el señor Schrems no impugna ni la Directiva 95/46/CE ni la Decisión 520/2000/CE sino el propio régimen de Puerto Seguro[24], pero a pesar de ello, el tribunal irlandés considera que la cuestión que se suscita es si, en virtud del artículo 25, apartado 6, de la Directiva 95/46/CE, la Autoridad de protección de datos irlandesa estaba vinculada por la constatación realizada por la Comisión Europea en la citada Decisión, según la cual el *Safe Harbour* (ya que la Decisión sólo reconoce el nivel adecuado del Acuerdo de Puerto Seguro, pero no de los EEUU)[25] garantiza un nivel de protección adecuado o si el artículo 8

24. Álvarez Hernando explica que «El Acuerdo de Puerto Seguro consta de siete principios básicos, complementados con una serie de "preguntas más frecuentes", básicamente referidas a tipos específicos de datos o tratamientos. Mediante este acuerdo, las empresas de los EEUU que se adhieran a él (sólo éstas y no sus filiales en otros países), cuentan con la presunción de adecuación al nivel de protección establecido por la Directiva 95/46/CE. Se trata, en definitiva, de un sistema voluntario de adhesión y autocertificación, pero no por ello, las empresas adheridas vienen obligadas a su cumplimiento efectivo. Algo muy criticable, pero sin duda, un gran avance en la difícil relación con EEUU, en el marco del flujo transfronterizo de datos». Álvarez Hernando, J., *Guía práctica sobre Protección de Datos: cuestiones y formularios*, Lex Nova, España, 2011. p. 429.

25. Como indica, al respect, Howard, cabe señalar que «Because the EU has determined that the United States not ensure an adequate level of protection, companies use other mechanisms to demonstrate that their systems do provide for adequate protections. In particular, the U.S. Department of Commerce offers a "safe harbor" program negotiated with the EU […] through which participating U.S. companies may be deemed to provide adequate data protection to allow them to receive transfers of personal data from the EU after they self-certify that they are compliant with the Safe Harbor Agreement´s provisions». Lo que puede traducirse como «Debido a que la Unión Europea ha determinado que los Estados Unidos no garantizan un nivel adecuado de protección, las empresas utilizan otros mecanismos para demostrar que sus sistemas no prevén protecciones adecuadas. En particular, el Departamento de Comercio de Estados Unidos ofrece un programa de "puerto seguro" negociado con la UE […] a través del cual las empresas americanas participantes pueden ser consideradas para proporcionar una protección adecuada de los datos que les permitan recibir transferencias de datos personales desde la UE después de haber autocertificado

de la Carta autorizaba a la *Data Protection Commissioner* a separarse de dicha constatación de la Comisión Europea.

El TJUE estima que la existencia de una Decisión de la Comisión Europea que declara que un país tercero garantiza un nivel de protección adecuado de los datos personales transferidos no puede dejar sin efecto ni limitar las facultades de las que disponen las autoridades nacionales de control en virtud de la Carta de los Derechos Fundamentales de la UE y de la Directiva 95/46/CE. Incluso ante una Decisión de la CE, las autoridades nacionales de control ante las que se haya presentado una solicitud, deben poder apreciar con toda independencia si la transferencia de los datos de una persona a un país tercero cumple las exigencias establecidas por la citada Directiva.

II. EL NIVEL EUROPEO DE PROTECCIÓN DE DATOS PERSONALES

1. LA CARTA DE LOS DERECHOS FUNDAMENTALES DE LA UNIÓN EUROPEA

En concreto, entrando ya en el análisis que hace el TJUE, en virtud de las dos cuestiones prejudiciales que le plantea la *High Court* irlandesa y que analiza de manera conjunta[26], dicho Tribunal comienza su sentencia[27] indicando que el objeto de la misma es interpretar, entre otras cuestiones, varios artículos de la Carta de los Derechos Fundamentales de la UE[28] entre los que se encuentran, el artículo 7, relativo al derecho a la vida privada[29] y, el artículo 8, relativo al derecho a la protección de datos de carácter personal[30].

Y dicha interpretación es necesaria ya que, en virtud de las consideraciones que hace la *High Court*, y que recoge el TJUE en su sentencia, «este asunto atañe a la aplicación del Derecho de la Unión, en el sentido del artículo 51[31] de la CDFUE por

---

que cumplen con las disposiciones del Acuerdo de Puerto Seguro». HOWARD, C. L., «The Organizational Ombudsman, Origins, Roles, and Operations A Legal Guide», *ABA*. p. 416.

26. Ver el apartado 37 de la sentencia.
27. Ver el apartado 1 de la sentencia.
28. Carta de los Derechos Fundamentales de la Unión Europea (*DOUE*, nº C, 326, de 26.10.2012).
29. Ya citado.
30. El artículo 8 de la CDFUE dice así: «1. Toda persona tiene derecho a la protección de datos de carácter personal que le conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación. 3. El respeto de estas normas estará sujeto al control de una autoridad independiente».
31. Apartado 34 de la sentencia. El artículo 51 de la CDFUE dice así «1. Las disposiciones de la presente Carta están dirigidas a las instituciones, órganos y organismos de la Unión, dentro del respeto del principio de subsidiariedad, así como a los Estados miembros únicamente cuando apliquen el Derecho de la Unión. Por consiguiente, éstos respetarán los derechos, observarán los principios y promoverán su aplicación, con arreglo a sus respectivas competencias y dentro de los límites de las competencias que los Tratados atribuyen a

lo que la legalidad de la Decisión 2000/520/CE de la Comisión relativa al Acuerdo de Puerto Seguro se analizará por dicho Tribunal a la vista, en particular, de «las exigencias derivadas […] de los artículos 7 y 8». Es así que las exigencias y garantías previstas en la CDFUE constituyen en este caso el estándar a considerar, en particular por lo que se refiere al derecho fundamental a la protección de datos personales de los ciudadanos europeos, el cual está estrechamente relacionado con la vida privada.

La atención se pone, precisamente, sobre la necesidad de que el TJUE analice la validez de la citada Decisión a la luz del Derecho de la Unión y, en particular, de los derechos a la vida privada y a la protección de datos personales, en la medida en que permite una injerencia por las autoridades públicas estadounidenses. Tal y como recoge el TJUE, cabe señalar que «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 quedaría privado de alcance alguno 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 de prevención de la delincuencia ligadas específicamente a los individuos afectados, y sin que esas prácticas se rodeen de garantías adecuadas y comprobables»[32].

Y lo anterior da lugar a que el TJUE, en el momento de comenzar con su posicionamiento sobre las cuestiones prejudiciales, señale que «se debe recordar previamente 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 protegidos por la Carta»[33] lo que significa, como explica más adelante, que «las normas de la Unión en materia de protección de las personas físicas respecto al tratamiento de datos personales»[34], en este caso, la citada Directiva, sean interpretadas a la luz, en particular, de los artículos 7 y 8 de la CDFUE.

La supremacía de la CDFUE, dado que se trata de Derecho primario de la UE[35], es una de las claves a tener en consideración en el presente caso, ya que las normas de la Unión en materia de protección de las personas físicas respecto al tratamiento de sus datos personales han de entenderse a la luz de los derechos fundamentales y los principios establecidos en dicha Carta, que se convierten en claras obligaciones y en el nivel de protección adecuada que debe garantizarse a los ciudadanos de la

---

la Unión. 2. La presente Carta no amplía el ámbito de aplicación del Derecho de la Unión más allá de las competencias de la Unión, ni crea ninguna competencia o misión nuevas para la Unión, ni modifica las competencias y misiones definidas en los Tratados».

32. Apartado 34 de la sentencia.

33. Apartado 38 de la sentencia.

34. Apartado 40 de la sentencia.

35. En cuanto al derecho primario y derivado de la Unión, puede verse Borchardt, K., *El ABC del Derecho de la Unión Europea*, Unión Europea, Luxemburgo, 2011.

Unión Europea, incluso cuando sus datos personales son transferidos a un tercer país.

Al respecto, cabe señalar que no es la primera vez, ni probablemente será tampoco la última, en la que el TJUE se pronuncia sobre el contenido y alcance de la CDFUE en cuanto a los derechos a la vida privada y a la protección de datos personales dada su relevancia. Y así lo afirma el TJUE, citando varias sentencias a lo largo de los últimos años, al señalar que «La jurisprudencia del Tribunal de Justicia destaca la importancia tanto del derecho al respeto de la privada garantizado por el artículo 7 de la Carta como del derecho fundamental a la protección de los datos personales que garantiza el artículo 8 de ésta (véanse las STJ, de 7.5.2009, as. Rijkeboer, (C-553/07), apartado 47; STJ, de 8.5.2014, as. Digital Rights Ireland y otros (C-293/12 y C-594/12), apartado 53, y STJ, de 14.5.2014, as. Google Spain y Google (C-131/12), apartados 53, 66 y 74)»[36].

Es decir, la CDFUE, y en particular los citados artículos, van a ser en el presente caso el instrumento de referencia que va a aplicar el TJUE para analizar si la Decisión 2000/520/CE es inválida, lo que supondría una vulneración del derecho a la protección de datos personales frente a su tratamiento en lo que se refiere al respeto de su vida privada. El hecho de interpretar también la Directiva 95/46/CE sobre protección de datos personales[37], en cuanto al régimen de las transferencias internacionales de datos como al papel de las autoridades de control, a la luz de la CDFUE, deja claro que de lo que se trata es de garantizar el derecho fundamental a la protección de datos personales, reconocido en el artículo 8 de la misma, a través de un nivel de protección adecuada que permita alcanzar, a su vez, un alto o elevado nivel de protección, en particular, del derecho a la protección de datos personales y, por extensión, de la vida privada así como de los derechos y libertades fundamentales de las personas.

Los derechos fundamentales consagrados en la CDFUE serán, por tanto, el parámetro que seguirá el TJUE para evaluar el grado de protección que ofrece la Decisión 2000/520/CE sobre el tratamiento de datos personales que se transfiere desde la Unión Europea.

2. LA INTERPRETACIÓN DEL DERECHO DE LA UE CONFORME A LA CARTA DE DERECHOS FUNDAMENTALES DE LA UE

Como ya hemos indicado, este caso, siguiendo así su propia línea jurisprudencial, el TJUE pone de manifiesto e insiste, una vez más, en que las normas de la Unión en materia de protección de las personas físicas respecto al tratamiento de los datos personales tienen que interpretarse conforme a los derechos fundamentales previstos en la CDFUE, que por lo que aquí interesa son tanto el de la vida privada como el de la protección de datos personales. Y la interrelación entre ambos derechos

36. Apartado 39 de la sentencia.

37. Ver el apartado 66 de la sentencia.

es clara, en tanto que la Directiva 95/46/CE regula, a través de sus disposiciones, «el tratamiento de datos personales, que puede vulnerar las libertades fundamentales y, en particular, el derecho al respeto de la vida privada»[38].

A pesar de que, como se indica expresamente en la sentencia, el recurrente ante la *High Court* «no haya impugnado formalmente la validez de la Directiva 95/46/CE ni de la Decisión 2000/520/CE»[39], en virtud de las cuestiones prejudiciales planteadas por ésta, el TJUE entra a analizar tanto la Directiva 95/46/CE sobre protección de datos personales[40] como la Decisión 2000/520/CE aprobada por la Comisión Europea en virtud del artículo 25, apartado 6, de dicha Directiva europea, conforme a las exigencias y garantías previstas en la CDFUE con respecto a los derechos a la vida privada y a la protección de datos de carácter personal.

Al respecto, el TJUE se refiere a la Directiva 95/46/CE y afirma que «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» y cita varias sentencias al respecto[41].

En concreto, por lo que se refiere al derecho a la protección de datos de carácter personal, el TJUE, mencionando los considerandos 2 y 10 así como el artículo 1 de la Directiva 95/46/CE recuerda que, en lo esencial, su objetivo es garantizar «una protección eficaz y completa de las libertades y de los derechos fundamentales de las personas físicas frente al tratamiento de los datos personales», de manera que dicha protección permita o sirva para alcanzar «un elevado nivel de protección de esas libertades y derechos fundamentales»[42].

En relación con lo anterior, cuando los datos personales son transferidos a un tercer país fuera de la Unión Europea (UE), incluyendo el Espacio Económico Europeo (EEE), como ocurre en el presente caso en el marco del Acuerdo de Puerto Seguro, se requiere que exista un nivel adecuado, ya que de lo contrario podría producirse una situación en la que la persona deje de estar protegida en sus derechos.

Esta protección de la persona frente al tratamiento de sus datos personales para garantizar su derecho a la vida privada tiene que darse a lo largo de todo el tratamiento de los datos personales, incluso cuando éstos salen del territorio de la Unión Europea, momento en el que entra en juego el nivel de protección adecuada o nivel adecuado que exige un nivel equivalente como garantía para poder transferir datos personales desde la Unión Europea hacia un tercer país.

38. Apartado 38 de la sentencia.
39. Apartado 35 de la sentencia.
40. Ya citada.
41. Apartado 38 de la sentencia.
42. Apartado 39 de la sentencia.

Aunque no es esta la primera vez que el TJUE trata un asunto en el que está presente la cuestión relativa al nivel de protección adecuada[43] previsto en el artículo 25 de la Directiva 95/46/CE, sí es la primera vez en que se pronuncia específicamente al respecto recordando que dicho término no ha sido definido en la citada Directiva. Y explica la referencia establecida en el apartado 2 del citado artículo[44] en cuanto a que las «circunstancias» a las que se atenderá constituyen una lista abierta, siendo lo fundamental que, por una parte, «un tercer país garantice un nivel de protección adecuado en razón de su legislación interna o de sus compromisos internacionales» y, por otra parte, «el carácter adecuado del nivel de protección que ofrece un tercer país se ha de apreciar "a efectos de la protección de la vida privada o de las libertades o de los derechos fundamentales de las personas"»[45].

Esta última referencia es a la que atiende el TJUE para explicar qué se entiende por «nivel de protección adecuado» y, citando las conclusiones del Abogado General, manifiesta al respecto que debe entenderse «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»[46].

Un nivel de protección adecuado, como indica el TJUE «significa que no cabe exigir que un tercer país garantice un nivel de protección idéntico al garantizado en el ordenamiento jurídico de la Unión»[47], lo que en la práctica implica proporcionar un nivel equivalente o similar al requerido por el artículo 8 de la CDFUE, al que da cumplimiento «el artículo 25, apartado 6, de la Directiva 95/46»[48]. Y esto supone que haya que tener en consideración que el nivel de protección adecuado lo establece el artículo 8 de la CDFUE que implica una «obligación expresa de protección de los datos personales», a la que se da cumplimiento a través de lo exigido por el artículo de la Directiva 95/46/CE que busca «asegurar la continuidad del elevado nivel de protección en caso de transferencia de datos personales a un tercer país»[49].

En definitiva, el nivel de protección adecuada en el caso de las transferencias internacionales de datos a un tercer país que exige el artículo 8 de la CDFUE y que

---

43. Ver la sentencia del STJ, de 30.5.2006, as. Parlamento/Consejo (C-317/04 y C-318/04).
44. El apartado 2 del artículo 25 de la Directiva 95/46/CE dice así: «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».
45. Apartado 71 de la sentencia.
46. Ver el apartado 73 de la sentencia.
47. Apartado 73 de la sentencia.
48. Ver el apartado 72 de la sentencia.
49. Apartado 72 de la sentencia.

se instrumentaliza a través del artículo 25 de la Directiva 95/46/CE por lo que respecta al tratamiento de los datos personales, se ha de evaluar considerando las reglas aplicables del tercer país de que se trate «en razón de su legislación interna o de sus compromisos internacionales»[50], para «asegurar la continuidad del elevado nivel de protección»[51] por lo que respecta a los derechos y libertades fundamentales de las personas.

3. LÍMITES A LAS INJERENCIAS A LOS DERECHOS Y LAS LIBERTADES FUNDAMENTALES

Conforme a lo ya indicado anteriormente, una protección adecuada implica que todo tratamiento de datos personales tenga que realizarse conforme a los requisitos, que se concretan tanto en condiciones de licitud del tratamiento como en la existencia de una o varias autoridades de control independientes, previstos en el derecho europeo sobre la protección de datos personales. Es decir, es necesario que todo tratamiento de datos personales, siendo este un concepto amplio que incluye también las transferencias internacionales aunque estas no hayan sido definidas en la Directiva 95/46/CE, tiene que cumplir con las condiciones de licitud establecidas en ésta de manera que se garantice «la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la [vida privada], en lo que respecta al tratamiento de los datos personales», tal como indica en su artículo 1.

Y dicha protección adecuada significa que, como apuntaba la *High Court*, hay que considerar, en particular, que «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 irlandesa»[52].

En este mismo sentido, el TJUE explica también que es necesario, en aquellos casos en los que los datos personales son transferidos a un tercer país, que «[a]unque los medios de los que se sirva este tercer país para garantizar ese nivel de protección pueden ser diferentes de los aplicados en la Unión para garantizar el cumplimiento de las exigencias derivadas de esta Directiva [95/46] entendida a la luz de la Carta, deben ser eficaces en la práctica para garantizar una protección sustancialmente equivalente a la garantizada en la Unión»[53].

Sin perjuicio de que la atención se ponga, en particular, en «el contenido de las reglas aplicables en ese país, derivadas de la legislación interna o de los compromisos internacionales de éste»[54], en el presente caso la inexistencia de un nivel adecuado se constata, según el TJUE, por el hecho de que los principios y requisi-

50. Apartado 71 de la sentencia.
51. Apartado 72 de la sentencia.
52. Apartado 33 de la sentencia.
53. Ver apartado 74 de la sentencia.
54. Ver el apartado 75 de la sentencia.

tos establecidos por el Acuerdo de Puerto Seguro «son aplicables únicamente a las entidades estadounidenses autocertificadas que reciban datos personales desde la Unión, sin que se exija que las autoridades públicas estadounidenses se sometan a esos principios»[55].

Esto lleva al TJUE a analizar el alcance de la excepción prevista en el anexo I, párrafo cuarto, de la Decisión 2000/520/CE ya que en su opinión hace posibles «injerencias fundadas en exigencias concernientes a la seguridad nacional, el interés público y el cumplimiento de la ley de Estados Unidos, en los derechos fundamentales de las personas cuyos datos personales se transfieren o pudieran transferirse desde la Unión Europea a Estados Unidos»[56]. Y continua explicando que a efectos de demostrar la injerencia en el derecho fundamental a la vida privada como consecuencia de la transferencia internacional es indiferente, por una parte, que los datos personales sean sensibles o no, y, por otra parte, que los interesados hayan sufrido o no inconvenientes en razón de tal injerencia[57].

Es así que el TJUE considera 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 […] que estuvieran autorizadas a llevar a cabo entidades estatales de ese país cuando persigan fines legítimos, como la seguridad nacional»[58]. Es decir, perseguir fines legítimos es un interés común, que tiene que llevarse a cabo con sujeción a los límites previstos para evitar injerencias indebidas por las autoridades públicas.

Para poder entender este razonamiento del TJUE, es necesario recordar que el apartado 2, del artículo 8, del Convenio de Derechos Humanos de la Unión Europea[59] (CEDH), relativo a la vida privada, y que la CDFUE tiene como referencia, prohíbe toda «injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás».

Y el TJUE se basa también en la constatación de la propia Comisión, a través de la Comunicación COM (2013) 846 final[60] y de la Comunicación COM (2013)

55. Ver el apartado 82 de la sentencia.

56. Apartado 87 de la sentencia.

57. Apartado 87, ya citado. Además, cita en este sentido la STJ, de 8.4.2014, as. Digital Rights Ireland y otros (C-293/12 y C-594/12), apartado 33.

58. Ver el apartado 88 de la sentencia.

59. Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales, Roma, 4.11.1950.

60. Ya citada.

847 final[61], sobre que «las autoridades estadounidenses podían acceder a los datos personales transferidos a partir de los Estados miembros a Estados Unidos y tratarlos de manera incompatible con las finalidades de esa transferencia, que va más allá de lo que era estrictamente necesario y proporcionado para la protección de la seguridad nacional»[62].

En este sentido, el TJUE recuerda, que tal y como ha desarrollado a través de su propia jurisprudencia, el «nivel de protección de las libertades y de derechos fundamentales garantizado en la Unión» implica que 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 de sus datos personales contra los riegos de abuso y contra cualquier acceso o utilización ilícitos de éstos»[63].

Se trata, en este caso, de garantizar el «derecho fundamental al respeto de la vida privada al nivel de la Unión»[64], lo que implica que resulte incompatible el hecho de que «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 a 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»[65].

En definitiva, cabe concluir, a la vista de la argumentación del TJUE que se basa en su jurisprudencia previa y sin perjuicio de considerar también otros aspectos tales como la posibilidad de que el justiciable ejerza acciones en Derecho para acceder a sus datos personales u obtener su rectificación o supresión, que una injerencia en las libertades y derechos fundamentales garantizados en la Unión, que ni esté justificada en virtud de reglas claras y precisas ni sea estrictamente necesaria y proporcionada (para la protección de la seguridad nacional) vulnera los derechos fundamentales a la vida privada y a la protección de datos personales consagrados en la CDFUE.

---

61. 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, COM (2013) 847 fina, Bruselas, 27.11.2013.
62. Ver el apartado 90 de la sentencia.
63. Ver el apartado 91 de la sentencia.
64. Apartado 92 de la sentencia.
65. Ver el apartado 93 de la sentencia.

III. ALCANCE DE LAS FACULTADES DE LAS AUTORIDADES DE PROTECCIÓN DE DATOS

1. FIGURA Y FUNCIONES DE LAS AUTORIDADES DE PROTECCIÓN DE DATOS CONFORME AL ARTÍCULO 28 DE LA DIRECTIVA 95/46/CE

En lo relativo a las facultades de las autoridades nacionales de control, en materia de transferencias de datos personales a terceros países fuera de la UE, el TJUE afirma que el artículo 28, apartado 1 de la Directiva 95/46/CE impone a los Estados miembros la obligación de instituir una o varias autoridades públicas encargadas del control, y actuando de forma independiente, del cumplimiento de la normativa de la UE en materia de protección de datos de las personas físicas respecto al tratamiento de datos personales. Dicha exigencia de contar con autoridades de control en materia de protección de datos en cada Estado miembro deriva no sólo del citado artículo de la Directiva 95/46/CE sino también del Derecho primario de la UE, en particular el artículo 8, apartado 3 de la CDFUE[66] y del artículo 16 TFUE, apartado 2[67]. La jurisprudencia de la UE así lo ha constatado también[68].

Las autoridades de control disponen de una gran variedad de facultades que el artículo 28, apartado 3, enumera de forma no exhaustiva por el artículo 28 de la citada Directiva y, según destaca el considerando 63 de la Directiva 95/46/CE[69], cuentan a su vez con diversos medios para el desarrollo de dichas facultades[70]. Por su parte, en cuanto a la acotación territorial de las facultades de las autoridades de control nacionales, el TJUE resalta que se limitan al territorio del Estado miembro en cuestión, no teniendo por tanto potestad para ejercer dichas facultades en un tercer país. Entre otras, estaría la facultad de investigación, recabando toda la información necesaria para el cumplimiento de su actividad de control, de facultades efectivas de intervención, como la de prohibir provisional o definitivamente un tratamiento de datos, o la capacidad para comparecer en juicio.

---

66. Art. 8.3 CDFUE: «El respeto de estas normas quedará sujeto al control de una autoridad independiente».

67. Art. 16 TFUE, apartado 2: «El Parlamento Europeo y el Consejo establecerán, con arreglo al procedimiento legislativo ordinario, las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal por las instituciones, órganos y organismos de la Unión, así como por los Estados Miembros en el ejercicio de las actividades comprendidas en el ámbito de aplicación del Derecho de la Unión, y sobre la circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes. […]».

68. Ver la STJ, de 16.10.2012, as. Comisión/Austria (C-614/10), apartado 36; así como la STJ, de 8.4.2014, as. Comisión/Hungría (C-288/12), apartado 47.

69. El considerando 63 de la Directiva 95/46/CE destaca: «Considerando que dicha autoridad debe disponer de los medios necesarios para cumplir su función, ya se trate de poderes de investigación o de intervención, en particular en casos de reclamaciones presentadas a la autoridad o de poder comparecer en juicio; que tal autoridad ha de contribuir a la transparencia de los tratamientos de datos efectuados en el Estado Miembro del que dependa».

70. Al respecto, en el ámbito de la UE, véase la STJ, de 1.10.2015, as. Weltimmo (C-230/14).

El TJUE destaca asimismo que autoridad 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/CE. Por su parte, el artículo 25 de la Directiva impone diversas obligaciones a los Estados miembros y a la Comisión Europea para controlar las transferencias de datos personales a terceros países en función del nivel de protección atribuido a éstos en cada uno de esos países. El TJUE destaca que, del propio artículo 25, 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 Europea[71].

La garantía de independencia de las autoridades de control nacionales es clave, según destaca el TJUE en el apartado 41 de la sentencia, garantía que se ha establecido para «reforzar la protección de las personas y de los organismos afectados por dichas decisiones», tal y como se destaca en el considerando 62 de la Directiva 95/46/CE[72] y en la jurisprudencia comunitaria[73]. A este respecto, P. L. Murillo de la Cueva y J. L. Piñar Mañas, insisten en que el principio de control independiente es uno de los principios inherentes a la protección de datos de carácter personal y autodeterminación informativa[74].

Los destinatarios de una Decisión de la CE en la que se garantice que un tercer país cumple con los niveles de exigencia de la normativa europea son los Estados miembros (conforme al párrafo segundo del artículo 25) y son éstos quienes deben adoptar las medidas necesarias para atenerse a ella. En virtud del artículo 288 TFUE dicha Decisión tiene carácter obligatorio para todos los Estados miembros y vincula, por tanto, a todos sus órganos.

El TJUE recuerda que las transferencias internacionales de datos de carácter personal tienen que hacerse con pleno respeto de lo dispuesto en la citada Directiva, en concreto con lo dispuesto en el Capítulo IV, donde se encuentran los artículos 25 y 26, «donde se establece un régimen dirigido a garantizar un control por los Estados Miembros de las transferencias de datos personales hacia terceros países», régimen que en todo caso complementa al capítulo II de la citada Directiva donde se establecen las condiciones generales de licitud de los tratamientos de datos personales[75].

---

71. Ver asimismo el punto 88 de las conclusiones del abogado general de 23 de septiembre de 2015.

72. Considerando 62 de la Directiva 95/46/CE: «Considerando que la creación de una autoridad de control que ejerza sus funciones con plena independencia de cada uno de los Estados Miembros constituye un elemento esencial de la protección de las personas en lo que respecta al tratamiento de datos personales».

73. STJ, de 9.3.2010, as. Comisión/Alemania (C-518/07), apartado 25. Ver asimismo STJ, de 8.4.2014, as. Comisión/Hungría (C-288/12), apartado 51.

74. Murillo de la Cueva, P. L. y Piñar Mañas, J. L., *El derecho a la autodeterminación informativa*, Fundación Coloquio Jurídico Europeo, Madrid, España, 2009, p. 104.

75. Ver apartado 46 de la sentencia, donde se hace referencia explícita a la STJ, de 6.11.2003, as. Lindqvist (C-101/01), apartado 63.

Es importante destacar que la función de revisar y examinar, de forma independiente, que tienen las autoridades de protección de datos de carácter personal, si un determinado país garantiza un nivel de protección adecuado, confirma algo que ya figura en el Tratado de Funcionamiento de la UE, que es que entre sus funciones, el TJUE tiene el control de la legalidad de los actos de las instituciones de la UE, incluyendo las Decisiones de la Comisión, lo que requiere que dicha legalidad pueda ser cuestionada no sólo por las autoridades de protección de datos de los Estados Miembros sino por los propios Estados miembros y otras instituciones. No obstante, queda claro que invalidar una Decisión de la Comisión sobre el nivel adecuado de un tercer país es una competencia exclusiva del TJUE.

2. EL PAPEL DE LAS AUTORIDADES DE PROTECCIÓN DE DATOS EN EL FUNCIONAMIENTO DEL ACUERDO DE PUERTO SEGURO

El artículo 3, apartado 1, párrafo primero, de la Decisión 2000/520/CE[76] establece una regulación específica de las facultades de las que disponen las autoridades nacionales de control ante una constatación por parte de la CE sobre el nivel de protección adecuado en un tercer Estado de fuera de la UE. A este respecto, el TJUE recuerda[77] que «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 […], 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».

Para el TJUE, este artículo tercero de la Decisión 520/2000/CE 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/CE, 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 con la protección de la vida privada de las personas. Además, recuerda 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

76. El art. 3, apartado 1, párrafo primero, de la Decisión 520/2000/CE apunta: «Transparencia de las políticas de protección de la vida privada de las entidades participantes. Según la pregunta más frecuente nº 6 anexa a la Decisión de Puerto Seguro (anexo II), las entidades interesadas en certificar su adhesión a los principios de Puerto Seguro tienen que facilitar al Departamento de Comercio su política de protección de la vida privada y hacerla pública, incluyendo su compromiso de adherirse a los principios. El requisito de hacer públicas las políticas de la vida privada de las entidades autocertificadas, al igual que su declaración de adhesión a los principios de privacidad, son fundamentales para el funcionamiento del sistema».

77. Ver apartado 101 de la sentencia del TJUE.

al respeto de la vida privada garantizado por el artículo 7 CDFUE[78], según jurisprudencia comunitaria[79].

Asimismo, el TJUE destaca que la facultad de ejecución atribuida a la Comisión por el legislador de la UE en el artículo 25, apartado 6, de la Directiva 95/46/CE, no confiere a la Comisión Europea la competencia para restringir las facultades de las autoridades nacionales de control.

Por tanto, tal y como señala el TJUE, una autoridad nacional de protección de datos está capacitada para, si bien no para declarar la invalidez de una Decisión de Puerto Seguro, por ser una competencia exclusiva que corresponde a dicho Tribunal, sí para cuestionar si pese a ella, se dan los requisitos necesarios para garantizar un nivel de protección adecuado, teniendo, por tanto, una función revisora y de control. Asimismo, puede suspender la transferencia en caso de que tenga dudas de que efectivamente se den esas garantías y dirigirse a los tribunales nacionales para que planteen una cuestión prejudicial.

3. DELIMITACIÓN Y COORDINACIÓN DEL EJERCICIO DE LAS FACULTADES DE LA COMISIÓN EUROPEA Y LAS AUTORIDADES DE PROTECCIÓN DE DATOS

La sentencia del TJUE aborda la delimitación y coordinación de funciones entre Autoridades de protección de datos de los países de la UE y la propia Comisión Europea, aspecto clave en la resolución de este caso, dadas las cuestiones prejudiciales planteadas.

El propio artículo 25 de la Directiva impone obligaciones tanto a la Comisión como a las autoridades de protección de datos de los Estados Miembros y, por ello, tal y como destacó el Abogado General en sus conclusiones[80], la constatación de si un tercer Estado garantiza un nivel de protección adecuado.

Con fundamento en el artículo 25, apartado 6 de la Directiva, la Comisión puede adoptar una Decisión que constate que un tercer país garantiza un nivel de protección adecuado, decisión que tiene carácter obligatorio para todos los Estados miembros vinculando a todos sus órganos, mientras dicha Decisión no haya sido declarada inválida por el TJUE, único órgano capaz de invalidar una Decisión de dicha índole. Si bien los tribunales nacionales están facultados para examinar la validez de un acto de la UE, carecen de competencia para declarar por sí mismos la invalidez de dicho acto. Además, como acto de una institución de la UE, una Decisión de esas características disfruta de la presunción de legalidad, produciendo efectos jurídicos mientras no haya sido o bien revocados, bien anulados mediante recurso de anulación o bien declarados inválidos al hilo de una cuestión prejudicial o una excepción de ilegalidad.

78. Apartado 94 de la sentencia.

79. STJ, de 8.4.2014, as. Digital Rights Ireland y otros (C-293/12 y C-594/12), apartado 52.

80. Ver apartado 88 de las conclusiones del abogado general.

El TJUE deja claro en su argumentación que el hecho de que la CE haya constatado, a través de una Decisión, que un determinado país garantiza un nivel de protección adecuado, no impide a las autoridades de control de los países de la UE examinar si dicho Estado cumple con las garantías necesarias para garantizar dicha protección, debiendo realizar dicha investigación cuando reciben una solicitud por parte de un ciudadano, pudiendo éste acudir a los órganos jurisdiccionales en caso de recibir una negativa por parte de la autoridad de control. Es más, en caso de apreciar que no se cumplen dichas garantías, la autoridad correspondiente está obligada a suspender la transferencia y, en su caso, el órgano jurisdiccional plantear una cuestión prejudicial. Por su parte, el TJUE aprecia que esa facultad de suspensión de los flujos de datos hacia una entidad que haya autocertificado su adhesión a los principios de la Decisión 520/2000/CE, es con carácter restrictivo, de acuerdo con el artículo 3 de la citada Decisión, de modo que sólo es posible la intervención a partir de un alto umbral de condiciones[81].

IV. LA DECISIÓN 2000/520/CE SOBRE EL ACUERDO DE PUERTO SEGURO

1. ANÁLISIS DEL TJUE SOBRE LA VALIDEZ DE LA DECISIÓN 2000/520/CE

Continuando con su análisis de la Decisión 2000/520/CE, el TJUE centra la atención en la validez de la misma a la luz de los requisitos establecidos en el artículo 25, apartado 6, de la Directiva 95/46/CE se pronuncia, específicamente, sobre los artículos 1 y 3 de dicha Decisión. Y, a su vez, el articulado de la Directiva 95/46/CE debe interpretarse, como afirma el Tribunal y por los motivos ya explicados, conforme a la CDFUE.

Antes de presentar las consideraciones que hace el TJUE sobre la validez del acto de ejecución de la Comisión, cabe señalar que la citada Decisión no incluye en su articulado ninguna previsión sobre una posible invalidez de parte (ni tampoco de la totalidad) de la misma, lo que en última instancia supone en este caso que la invalidez de dos artículos afecte por completo a todo el articulado.

Por lo que se refiere al artículo 1 de la Decisión 2000/520/CE, relativo a los principios del Acuerdo de Puerto Seguro y a la adhesión a los mismos por organizaciones

81. El apartado 101 de la sentencia destaca, en relación con el artículo 3 de la Decisión 520/2000: «De esa forma, a tenor de dicha disposición las referidas autoridades, 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, […] podrán ejercer su facultad de suspender los flujos de datos hacia una entidad que haya autocertificado su adhesión a los principios [de la Decisión 520/2000], de manera restrictiva, ya que sólo es posible la intervención a partir de un alto umbral de condiciones. Aunque esa disposición no enerva las facultades de esas autoridades para tomar medidas encaminadas a asegurar el cumplimiento de las disposiciones nacionales adoptadas en aplicación de esa Directiva, excluye en cambio la posibilidad de que esas autoridades tomen medidas con objeto de asegurar el cumplimiento del artículo 25 de la misma Directiva».

estadounidenses sujetas a la jurisdicción de la Comisión Federal de Comercio (*Federal Trade Commission*, FTC) o del Departamento de Transportes (*US Department of Transportation*), en los términos previstos en la Decisión, el TJUE se basa en que estos principios no se aplican a «las autoridades públicas estadounidenses»[82] y que las mismas pueden acceder a los datos personales de los ciudadanos europeos sin limitación alguna en virtud de una excepción de carácter general relativa a que «La adhesión a estos principios puede limitarse: a) cuanto sea necesario para cumplir las exigencias de seguridad nacional, interés público y cumplimiento de la ley»[83].

La referida excepción a los principios sería aceptable de darse algunas garantías, pero como explica el TJJUE, en este caso la «Decisión 2000/520 no contiene ninguna constatación sobre la existencia en Estados Unidos de reglas estatales destinadas a limitar posibles injerencias»[84], y tampoco «pone de manifiesto la existencia de una protección jurídica eficaz contra injerencias de esa naturaleza»[85], por lo que al no haber «reglas claras y precisas que regulen el alcance y la aplicación de una medida e impongan exigencias mínimas» para proteger a la persona frente al tratamiento de sus datos personales que pueda suponer «riesgos de abuso y contra cualquier acceso o utilización ilícitos de éstos»[86], implica que se exceda de lo «estrictamente necesario» y proporcionado.

Unido a lo anterior, tampoco se garantiza el derecho a la tutela judicial efectiva, previsto en el artículo 47 de la CDFUE[87], a través de «vías jurídicas administrativas o judiciales que les permitan acceder a los que les concernían y obtener, en su caso, su rectificación o supresión»[88].

Además, el TJUE aprecia que la Comisión no constató, de manera debidamente motivada, que el tercer país, en este caso Estados Unidos, proporciona un nivel adecuado, tal como exige el artículo 25, apartado 6, de la Directiva 95/46/CE. Ahora bien, la Decisión 2000/520/CE no es sobre Estados Unidos, siendo relevante el hecho de que el TJUE señale expresamente que «se ha de observar que 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»[89]. Es decir, el nivel adecuado en este caso, se aplicaba al Acuerdo de Puerto Seguro lo que requería cumplir con las exigencias previstas en la Directiva 95/46/CE a la luz de la CDFUE de manera que tienen que garantizarse los

82. Ver el apartado 82 de la sentencia.
83. Ver el Anexo I, párrafo cuarto, de la Decisión 2000/520/CE y el apartado 87 de la sentencia.
84. Ver el apartado 88 de la sentencia.
85. Apartado 89 de la sentencia.
86. Ver el apartado 91 de la sentencia.
87. El primer párrafo del artículo 47 de la CDFUE dice así: «Toda persona cuyos derechos y libertades garantizados por el Derecho de la Unión hayan sido violados tiene derecho a la tutela judicial efectiva respetando las condiciones establecidas en el presente artículo».
88. Ver los apartados 90 y 95 de la sentencia.
89. Ver el apartado 97 de la sentencia.

derechos y libertades fundamentales de los ciudadanos de la UE, por lo que las excepciones previstas en el mismo resultan incompatibles con el derecho fundamental a la protección de datos personales de los ciudadanos europeos.

Y todo lo anterior, sin que el TJUE analice ya el contenido de los principios, lleva a éste a concluir que el artículo 1 de la Decisión es inválido porque «vulnera las exigencias establecidas por el artículo 25, apartado 6, de la Directiva 95/46, entendido a la luz de la Carta»[90].

El otro artículo de la Decisión 2000/520/CE que considera el TJUE al analizar su validez es el artículo 1, relativo a las facultades de las autoridades nacionales de protección de datos personales, prestando especial atención al apartado 1, párrafo primero[91].

Como ya hemos analizado al tratar la cuestión relativa a las facultades de las Autoridades de protección de datos, el TJUE considera que dicho artículo establece un «alto umbral de condiciones»[92] que las priva de «las facultades que les atribuye el artículo 28 de la Directiva 95/46»[93]. Esto implica también que el TJUE considere que la Comisión se ha excedido en sus facultades de ejecución, ya que el legislador de la Unión no le ha conferido, a la vista del artículo 25, apartado 6, de la Directiva 95/46/CE, «la competencia para restringir las facultades de las autoridades nacionales de control»[94].

No obstante, la conclusión del TJUE se basa en considerar que la Autoridad de protección de datos irlandesa no adoptó medidas «con toda la diligencia exigible»[95] cuando se le presentó una reclamación sobre la que es necesario y preciso recordar que fue rechazada por infundada. Es decir, aunque el TJUE llega a la conclusión ya apuntada tras su análisis de la Decisión 2000/520/CE, hay que considerar también que la autoridad de control irlandesa había desestimado por infundada la solicitud, sin responder que no fuese competente, tal y como parece apuntar el TJUE a pesar de que explica las diferentes situaciones que pueden darse en la práctica.

En cuanto al presente caso, sería también necesario tener en consideración que, aunque la sentencia se centra en que el artículo 3 de la Decisión 2000/520/

90. Ver el apartado 98 de la sentencia.

91. El apartado 1, párrafo primero, del artículo 3 de la Decisión 2000/520/CE dice así: «1. 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/CE, las autoridades competentes de los Estados miembros podrán ejercer su facultad de suspender los flujos de datos hacia una entidad que haya autocertificado su adhesión a los principios y su aplicación de conformidad con las FAQ, a fin de proteger a los particulares contra el tratamiento de sus datos personales, en los casos siguientes».

92. Ver el apartado 101 de la sentencia.

93. Ver el apartado 102 de la sentencia.

94. Apartado 103 de la sentencia.

95. Apartado 63 de la sentencia.

CE impone a las autoridades de protección de datos «un alto umbral de condiciones» para actuar y suspender transferencias internacionales de datos en el marco del Acuerdo de Puerto Seguro, el recurrente es un ciudadano austríaco que presentó su reclamación ante la Autoridad de protección de datos irlandesa, pero nada dice la sentencia y, por tanto, nada sabremos sobre qué hubiera ocurrido si este usuario de la red social hubiera presentado su reclamación no ante la autoridad del país donde la empresa responsable de la red está establecida en la Unión Europea, sino ante la de su país de residencia, es decir, Austria. Quizás sea esta una cuestión que requiere atender a otras sentencias del Tribunal[96] pero sobre la que hubiera sido deseable conocer el criterio del TJUE en cuanto a si los tribunales nacionales son los del país de residencia del recurrente o de aquél país de la autoridad de protección de datos ante el que se haya presentado la reclamación correspondiente.

Es decir, hubiera sido deseable que el TJUE se hubiera manifestado sobre esta cuestión atendiendo a que un ciudadano europeo decida acudir, por los motivos o razones que fuera, a una Autoridad de protección de datos personales que no sea la del país de residencia sino la del lugar de establecimiento de la organización que trata sus datos personales.

Los elementos presentes en este caso, en cuanto a que un ciudadano de la Unión Europea pueda dirigirse a la autoridad de protección de datos personales que considere oportuna, podría haber sido también objeto de un pronunciamiento específico del TJUE para dejar claro qué criterios seguir cuando un ciudadano presenta una reclamación ante una autoridad de control antes de expresar, sin más, que «incumbe a esa autoridad examinar la referida solicitud con toda la diligencia exigible»[97].

En virtud de la conclusión que alcanza el TJUE, sin necesidad de analizar nada más en relación con la Decisión 2000/520/CE y dado que «los artículos 1 y 3 […] son indisociables de los artículos 2 y 4 y de los anexos», declara que la misma «es inválida»[98].

2. INVALIDEZ Y CONSECUENCIAS

En cuanto a quién puede declarar la invalidez de un acto de Derecho de la Unión, es importante considerar, previamente y sin perjuicio de lo ya expuesto al respecto, que el TJUE dedica varios apartados[99] a explicar, quizás por si hubiera dudas al respecto, el reparto de competencias en cuanto a la declaración de invalidez de una decisión de la Comisión como la que es objeto del presente caso. En concreto, el TJUE indica que «es exclusivamente competente para declarar la invalidez de un acto de la Unión» ya que se trata de una «competencia exclusiva cuyo objeto es

96. Ver la STJ, de 1.10.2015, as. Weltimmo (C-230/14), ya citada.

97. Ver el apartado 63 de la sentencia.

98. Ver apartados 105 y 106 así como el fallo.

99. Véanse los apartados 61 y 62 de la sentencia.

garantizar la seguridad jurídica preservando la aplicación uniforme del Derecho de la Unión»[100].

Y a continuación explica, por lo que se refiere a los tribunales nacionales, que «están ciertamente facultados para examinar la validez de un acto de la Unión», pero que «carecen sin embargo de competencia para declarar ellos mismos su invalidez», y por lo que se refiere a las autoridades de control, recuerda que «no están habilitadas para declarar la invalidez de la referida decisión»[101].

Establecido lo anterior, por los motivos expuestos, y que hemos resumido de manera analítica, el TJUE expresa que «[t]oda vez que los artículos 1 y 3 de la Decisión 2000/520 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»[102] por lo que concluye que dicha decisión «es inválida»[103].

Con la declaración de invalidez de la Decisión 2000/520/CE, el TJUE cumple con sus competencias de manera que a partir de la sentencia es necesario atender a las que, a su vez, tengan atribuidas, en su caso, cada uno de los actores de la Unión Europea involucrados y lo que supone, en esencia, que la Comisión tenga que buscar un nuevo Acuerdo de Puerto Seguro a la vista del fallo del TJUE. A este respecto, la propia Comisión ha destacado la necesidad de que el nuevo acuerdo sea «comprehensivo» y con «compromisos legales claros»[104]. Por otra parte, y en lo que respecta a la negociación de un nuevo acuerdo, cabe destacar que desde un origen el acuerdo *Safe Harbour* ha sido concebido como un «proceso continuo»[105].

En cualquier caso, lo único que queda claro es que, con la declaración de invalidez del Acuerdo de Puerto Seguro, desaparece la posibilidad de que quienes transfieren datos personales desde la Unión Europea a una organización adherida al Acuerdo de Puerto Seguro en los Estados Unidos puedan recurrir a este mecanismo como base legal para proporcionar garantías suficientes a efectos de dicha transferencia internacional de datos. Es decir, quienes antes transferían datos personales desde la Unión Europea a las organizaciones adheridas al Acuerdo de Puerto Seguro sin necesidad de autorización, en su caso, ahora tendrán que obtenerla o recurrir a

100. Ver el apartado 61 de la sentencia.

101. Ver el apartado 62 de la sentencia.

102. Ver el apartado 105 de la sentencia.

103. Apartado 106 de la sentencia y punto 2 del fallo.

104. Discurso de la Comisaria de la CE Vera Jourová (*speech of Commissioner Jourová at Conference Digital Values: Advancing technology-preserving fundamental rights organised by Carnegie Europe and Microsoft*). La comisaria destacó (literal en inglés): «Only a comprehensive agreement with clear legal commitments can ensure the level of data protection Europeans are entitled to under EU Law. […] Where persona data travels, the protection has to travel with it in a system that it is equivalent».

105. Farrell, H.: «Negotiating privacy across arenas: The EU-US Safe Harbour discussions» en *Common Goods: Reinventing European and International Governance*, Ed. Adrienne Héritier, 2002, pp. 105-126.

alguna de las excepciones previstas en el apartado 1, del artículo 26, de la Directiva 95/46/CE a la prohibición de transferencias internacionales a terceros países sin nivel adecuado[106].

Ahora bien, el TJUE no aclara en su sentencia desde cuándo produce efectos la declaración de invalidez, en el sentido de si tiene o no efectos retroactivos. Cabría entender que la declaración de invalidez, al igual que ocurrió en el caso de la Directiva 2006/24/CE[107], produce efectos desde la fecha de entrada en vigor de la Decisión 2000/520/CE ya que el Tribunal no ha limitado en el tiempo los efectos de su sentencia[108].

Y otra de las consecuencias que se deriva de la declaración de invalidez de la Decisión mencionada es que, con carácter general, las autoridades nacionales de protección de datos, y en este caso concreto, la Autoridad irlandesa de protección de datos, como autoridad de control, tenga que examinar la reclamación que le fue planteada, investigar los hechos y, en virtud de los resultados, en el ejercicio de las atribuciones que tiene conferidas, decidir si procede, o no, suspender la transferencia internacional de datos de los usuarios de la red social desde la Unión Europea a los Estados Unidos al constatarse que dicho país no ofrece un nivel de protección adecuado de los datos personales de los ciudadanos europeos.

Por último, la declaración de invalidez supone, también, que la Comisión tenga que negociar con el Departamento de Comercio de los EEUU un nuevo Acuerdo de Puerto Seguro, así como ver en la práctica la uniformidad y efectividad en la actuación de las Autoridades europeas de protección de datos y la validez de futuras Decisiones de la Comisión.

V. CONCLUSIONES

1. El derecho a la protección de datos personales es un derecho fundamental en la Unión Europea, consagrado como un derecho autónomo en el artículo 8 de la Carta de los Derechos Fundamentales de la UE, aunque interrelacionado al mismo tiempo con otros derechos, como el derecho a la vida privada y el derecho a la tutela judicial efectiva, también incluidos en dicha Carta. Al respecto, todo el derecho derivado, tanto la Directiva 95/46/CE como la, aunque ya invalidada, Decisión 2000/520/CE, tienen que interpretarse conforme a dicha Carta, como derecho primario de la UE, de manera que los parámetros, en cuanto a las garantías

106. Ya citado.

107. Directiva 2006/24/CE, del Parlamento y del Consejo, de 15.3.2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicación electrónica de acceso público o de redes públicas de comunicación y por la que se modifica la Directiva 2002/58/CE (DOUE L105/54, de 13.4.2006).

108. Ver la STJ, de 8.5.2014, as. Digital Rights Ireland, ya citada, y otros.

exigibles para proteger los derechos fundamentales de los ciudadanos europeos, son los previstos en aquélla.

2. En materia de protección de datos personales la Directiva 95/46/CE, que debe interpretarse y aplicarse a la luz del derecho fundamental a la protección de datos personales consagrado en la Carta de los Derechos Fundamentales de la UE, implica que deba garantizarse un nivel de protección adecuada. Aunque la citada Directiva no define qué se entiende por protección adecuada, aplicada a terceros países implica que sea exigible un nivel sustancialmente equivalente de protección de los derechos y las libertades fundamentales frente a toda injerencia por autoridades públicas que no resulte de reglas claras y precisas, dando lugar así a un acceso que no sea «estrictamente necesario y proporcionado para la protección de la seguridad nacional»[109].

3. El TJUE estima que la existencia de una Decisión de la Comisión Europea que declara que un país tercero garantiza un nivel de protección adecuado de los datos personales transferidos no puede dejar sin efecto ni limitar las facultades de las que disponen las autoridades nacionales de control en virtud de la Carta de los Derechos Fundamentales de la UE y de la Directiva 95/46/CE. Incluso ante una Decisión de la CE, las autoridades nacionales de control ante las que se haya presentado una solicitud, deben poder apreciar con toda independencia si la transferencia de los datos de una persona a un país tercero cumple las exigencias establecidas por la Directiva, suspender en su caso la transferencia y dirigirse a los tribunales para que planteen una cuestión prejudicial.

4. En esta sentencia, el TJUE considera que el marco *Safe Harbour* entre EEUU y la UE podría dar lugar a «injerencias en los derechos fundamentales de las personas cuyos datos personales se transfieran desde la Unión a Estados Unidos». Además, recalca que las exigencias, basadas en reglas que según las conclusiones del TJUE no son claras ni precisas, de seguridad nacional, de interés público y cumplimiento de la ley de EEUU están por encima de los principios de Puerto Seguro.

5. En la práctica, la aplicación del fallo de la sentencia del TJUE genera inseguridad jurídica e incertidumbre con respecto a cómo deben realizar ahora las necesarias transferencias internacionales de datos entre la UE y EEUU, transferencias vitales en el comercio internacional. El marco *Safe Harbour* ha estado vigente desde hace 15 años y, en el momento en el que se produjo este fallo que invalida la Decisión 2000/520/CE se estaba negociando la revisión del marco. Por todo ello, tras la declaración de invalidez de la Decisión de la CE, la situación es de incertidumbre

109. Apartado 22 de la sentencia.

hasta que el WP 29 dicte unas *guidelines* o pautas claras para que los responsables y encargados de tratamiento sepan cómo efectuar las transferencias o bien hasta que se renegocie el acuerdo entre la Comisión Europea y los EEUU.

6. Este fallo jurisprudencial invita a cuestionarse la validez de otras Decisiones de la Comisión Europea en las que ha dejado constancia de que terceros países garantizan un nivel de protección adecuado (Argentina, Canadá, Suiza, etc…), así, hasta el total de 11 terceros países con los que existe un acuerdo de dichas características, reconocido a través las correspondientes Decisiones de la CE. Por ello, puede haber un número creciente de cuestiones prejudiciales que se planteen por tribunales de Estados Miembros de la UE en relación con Decisiones de la CE en las que se considera que terceros países tienen un nivel equivalente de protección de los datos de carácter personal.

7. En definitiva, se trata de una sentencia relevante, por lo que se refiere al derecho fundamental a la protección de datos, y transcendental, en cuanto a las cuestiones que plantea y que en aras de evitar situaciones de inseguridad jurídica y aplicaciones extremas, requiere que todos los actores involucrados, desde las Autoridades nacionales de protección de datos hasta la Comisión Europea, actúen armónicamente evitando cualquier situación que dé lugar a que la persona se vea desprotegida lo que, además, podría llegar a generar desconfianza que impacte negativamente en la posibilidad de ofrecer servicios tecnológicos que buscan cumplir con estándares internacionales de protección de datos a través de la adhesión a mecanismos como el *Safe Harbour*.