

## **JURISPRUDENCIA**

---



## DERECHOS FUNDAMENTALES VERSUS VIGILANCIA MASIVA

Comentario a la sentencia del Tribunal de Justicia (Gran Sala)  
de 6 de octubre de 2015 en el asunto C-362/14 *Schrems*

ELISA URÍA GAVILÁN<sup>1</sup>

*Revista de Derecho Comunitario Europeo*  
ISSN-L 1138-4026, núm. 53, Madrid, enero/abril (2016), pp. 261-282  
<http://dx.doi.org/10.18042/cepc/rdce.53.07>

**Cómo citar/Citation**

Uría Gavilán, E. (2016). Derechos fundamentales versus vigilancia masiva.  
*Revista de Derecho Comunitario Europeo*, 53, 261-282.  
doi: <http://dx.doi.org/10.18042/cepc/rdce.53.07>

### Resumen

La sentencia del Tribunal en el asunto *Schrems* declara la invalidez de la Decisión 2000/520 sobre los principios de puerto seguro, mediante la cual la Comisión Europea constataba que las transferencias de datos personales entre la Unión Europea y los Estados Unidos tenían un nivel de protección adecuado. El Tribunal invalida el acto normativo por dos razones: no respeta el «contenido esencial» de derechos fundamentales consagrados en la Carta (art. 7 y art. 47) y priva a las autoridades nacionales del poder de evaluar la solicitud de una persona que cuestiona la compatibilidad de esa Decisión con aquellos derechos. Asimismo, el Tribunal concluye que la Decisión no debe impedir que las autoridades nacionales examinen dichas solicitudes.

---

<sup>1</sup> Becaria de investigación predoctoral en el Departamento de Derecho Internacional, Eclesiástico y Filosofía del Derecho de la Universidad Carlos III de Madrid, con una beca de doctorado de la Fundación La Caixa. LLM Derecho Europeo, Colegio de Europa (Brujas).

**Palabras clave**

Puerto seguro; protección de datos; privacidad; Carta de Derechos Fundamentales de la Unión Europea; autoridades nacionales de control.

**FUNDAMENTAL RIGHTS VERSUS MASS SURVEILLANCE**

**Comment of the Judgment of the Court of Justice of the European Union (Grand Chamber) of 6th October of 2015, case C-362/14 Schrems**

**Abstract**

The judgment of the Court in the case *Schrems* declares Decision 2000/520 on the safe harbour principles whereby the Commission determined that a third country ensured an adequate level of protection invalid. The Court annuls the Decision on two grounds: it does not respect the «essential content» of fundamental rights enshrined in the Charter (articles 7 and 47) and it denies the national supervisory authorities the power to examine the claim of a person calling into question the compatibility of the Decision with those rights. Furthermore, the Court declares that the Decision does not prevent national authorities from examining those claims.

**Key words**

Safe harbour; data protection; privacy; Charter of the Fundamental Rights of the European Union; national supervisory authorities.

**LES DROITS FONDAMENTAUX VERSUS LA SURVEILLANCE DE MASSE**

**Commentaire de l'arrêt de la Cour de Justice de l'Union Européenne (Grand Chambre), 6 octobre 2015, affaire C-362/14 Schrems**

**Résumé**

L'arrêt de la Cour dans l'affaire *Schrems* déclare invalide la Décision 2000/520 relative aux principes de la «sphère de sécurité», dans laquelle la Commission constatait que les transferts des données à caractère personnel entre l'Union Européenne et les États Unis assuraient un niveau de protection adéquat. La Cour invalide l'acte normative par deux raisons: il ne respecte pas le contenu essentiel des droits fondamentaux consacrés dans la Charte (article 7 et article 47) et il prive les autorités nationales de contrôle d'examiner une demande où une personne remet en cause la compatibilité de la décision avec ces droits. En outre, la Cour considère que la décision n'empêche les autorités d'examiner ces demandes.

**Mots clés**

Sphère de sécurité; protection des données personnelles; vie privée; Charte des droits fondamentaux de l'Union européenne; autorités nationales de contrôle.

## SUMARIO

---

I. INTRODUCCIÓN. II. MARCO JURÍDICO: LA NORMATIVA DE PUERTO SEGURO. III. RESUMEN DE LOS HECHOS. IV. LA SENTENCIA DEL TRIBUNAL DE JUSTICIA. V. VALORACIÓN DE LA SENTENCIA: 1. Sobre la independencia de las autoridades nacionales de protección de datos; 2. La declaración de invalidez de la Decisión y la vulneración de derechos fundamentales. VI. CONSIDERACIONES FINALES.

---

### I. INTRODUCCIÓN

Nos encontramos ante uno de los asuntos más importantes del Tribunal de Justicia de la Unión (en lo sucesivo, «el Tribunal» o el «TJUE») de los últimos tiempos. Maximilian Schrems, un joven jurista usuario de redes sociales, emprendió una batalla legal contra Facebook, que ha concluido con la anulación de la Decisión de la Comisión que gobernaba la transferencia de datos personales entre la Unión y los Estados Unidos (el acuerdo de puerto seguro) desde hacía quince años. Se trata de un caso que refleja los desafíos de la era cibernética en la que vivimos y la consecuente necesidad de un tribunal garantista que equilibre la balanza entre la seguridad pública y las libertades fundamentales. En este sentido, es muy ilustrativa la declaración que el presidente del Tribunal de Justicia, Koen Lenaerts, realizaba cuando se le preguntó sobre este asunto: «*the rule of law is not up for sale*» (el Estado de derecho no está en venta)<sup>2</sup>. Así, el caso Scherms<sup>3</sup> se configura como una pieza esencial del

---

<sup>2</sup> Entrevista publicada en el *Wall Street Journal* el 14 de octubre de 2015, «ECJ President On EU Integration, Public Opinion, Safe Harbor, Antitrust» <http://blogs.wsj.com/brussels/2015/10/14/ecj-president-on-eu-integration-public-opinion-safe-harbor-antitrust/> (último acceso, 28 de diciembre de 2015).

<sup>3</sup> Sentencia del Tribunal de Justicia Schrems, C-362/14, EU:C:2015:650. Sobre esta decisión véase Sergio CARRERA y Elspeth GUILD, «Safe Harbour or into the storm? EU-US data transfers after the Schrems judgment», CEPS Paper in Liberty and Security in Europe núm. 85 / noviembre de 2015; M. Skrinjar VIDOVIC «Schrems v Data Protection Commissioner (Case C-362/14): Empowering National Data Protection Authorities», *Croatian Yearbook of European Law and Policy*, 2015. Sobre los hechos del caso antes de la sentencia del Tribunal, véase Shane DARCY, «Battling

mosaico de la salvaguardia de los derechos fundamentales en la Unión Europea y, más particularmente, del derecho a la privacidad y la protección de los datos personales.

## II. MARCO JURÍDICO: LA NORMATIVA DE PUERTO SEGURO

Es necesario hacer una breve referencia al contexto legislativo europeo de protección de datos para comprender esta sentencia<sup>4</sup>. La norma básica en este ámbito es la Directiva 95/46/CE 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<sup>5</sup> (en adelante, la «Directiva») que, entre muchas otras cuestiones, establece que solo se podrán transferir datos personales a aquellos países no comunitarios<sup>6</sup> que ofrezcan un nivel adecuado de protección de la vida privada<sup>7</sup>.

---

for the Rights to Privacy and Data Protection in the Irish Courts», *Utrecht Journal of International and European Law*, vol. 31, Issue 80, pp. 131-136.

<sup>4</sup> Por cuestiones de limitación de espacio, nos referiremos tan solo a la Directiva 95/46/CE y a la Decisión 2000/520, dado que son las piezas claves de este asunto. No obstante, conviene apuntar que nos encontramos en un momento crucial de cambio en la legislación europea de protección de datos, ya que dos actos normativos están en proceso de elaboración: el Reglamento General de Protección de Datos (puede verse la propuesta de la Comisión en: [http://ec.europa.eu/justice/data-protection/document/review2012/com\\_2012\\_11\\_es.pdf](http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_es.pdf) (último acceso 28 de diciembre de 2015) y la Directiva de protección de datos en materia de cooperación policial y judicial (puede verse la propuesta en <http://register.consilium.europa.eu/doc/srv?f=ST+5833+2012+INIT&l=es> (último acceso 28 de diciembre de 2015)).

<sup>5</sup> DO L 281, de 23 de noviembre de 1995, p. 31.

<sup>6</sup> Esa referencia comprende tanto el territorio de la Unión Europea, actualmente compuesta por 28 Estados miembros, como los países del Espacio Económico Europeo (Islandia, Liechtenstein y Noruega).

<sup>7</sup> Así lo expone el párrafo 1 del art. 25 que establece los «principios» de la Directiva: «1. Los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado».

¿Cómo sabemos que un país dispone de ese «nivel adecuado»? La Comisión Europea es la encargada de hacer constar que un país tercero<sup>8</sup> garantiza ese estándar de protección a través de dos elementos: la legislación interna de aquel o los compromisos internacionales que haya asumido<sup>9</sup>. En este contexto, la Comisión celebró un acuerdo con el Departamento de Comercio de Estados Unidos que constituye la piedra angular de este caso: el acuerdo de puerto seguro (*safe harbour*, en inglés), que el ejecutivo de la Unión materializó en la Decisión 2000/520/CE<sup>10</sup> (en lo sucesivo, la «Decisión»)<sup>11</sup>. Mediante esta norma, se implantó un sistema de autocertificación, es decir, se daba la posibilidad a las entidades estadounidenses<sup>12</sup> de adherirse a una lista de principios, conforme a los cuales se comprometían a gestionar los datos personales. Una vez adheridas al acuerdo de puerto seguro, las empresas disponían de una presunción de adecuación al nivel de protección exigido por la Directiva.

<sup>8</sup> Hasta la fecha, y aparte del acuerdo con Estados Unidos, la Comisión ha adoptado once decisiones por las que ha declarado que determinados países cuentan con un nivel similar de protección de datos y pueden hacerse transferencias sin autorización (Suiza, Canadá, Argentina, Guernsey, Isla de Man, Jersey, Islas Feroe, Andorra, Israel, Uruguay y Nueva Zelanda), como puede verse en el siguiente enlace: [http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index\\_en.htm](http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm) (último acceso 8 de enero de 2016).

<sup>9</sup> Art. 25.6 de la Directiva:

«La Comisión podrá hacer constar, de conformidad con el procedimiento previsto en el apdo. 2 del art. 31, que un país tercero garantiza un nivel de protección adecuado de conformidad con el apdo. 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 apdo. 5, a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas».

<sup>10</sup> Decisión de la CE, 2000/520/CE, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América (DO L 215/7, de 25 de agosto de 2000, p. 7).

<sup>11</sup> Véase un análisis exhaustivo de la Decisión puerto seguro en María ÁLVAREZ CARO y Miguel RECIO GAYO, «Hacia un acuerdo Safe Harbour renovado para la transferencia internacional de datos entre EEUU y la UE», *Working Papers on European Law and Regional Integration*, núm. 25, 2015.

<sup>12</sup> Estas eran aproximadamente 4.500 cuando se dictó la sentencia, según el informe del *Congressional Research Service* de Estados Unidos «The EU-U.S. Safe Harbor Agreement on Personal Data Privacy: In Brief», <https://www.fas.org/sgp/crs/misc/R44257.pdf> (último acceso 27 de diciembre de 2015).

Por otro lado, es importante señalar que la Directiva determina que cada Estado miembro tiene que designar una o varias autoridades públicas encargadas de controlar la aplicación en su territorio de las disposiciones nacionales adoptadas sobre la base de aquella. Se trata de las denominadas «autoridades nacionales de control»<sup>13</sup> (en adelante, las «autoridades») que adquieren un papel protagonista en este asunto.

### III. RESUMEN DE LOS HECHOS

La historia comenzó en junio de 2013, cuando Maximilian Scherms, un jurista austríaco usuario de Facebook, reclamó ante la autoridad irlandesa de protección de datos —el Comisario irlandés de protección de datos (en adelante, el «Comisario») — con la finalidad de que prohibiera a la filial de la red social, Facebook Ireland, transferir sus datos personales a Estados Unidos<sup>14</sup>. Este país se ve implicado en el asunto porque la filial irlandesa transmite la información de todos los usuarios residentes en la Unión Europea a los servidores de Facebook ubicados en Estados Unidos. El Sr. Scherms alegaba que el Derecho y las prácticas en vigor en aquel país no garantizaban una protección suficiente de los datos personales conservados en su territorio. Sustentaba sus sospechas en las revelaciones de Edward Snowden sobre la vigilancia masiva de los servicios de información estadounidenses, en particular, la llevada a cabo, supuestamente, por la National Security Agency («NSA»)<sup>15</sup>.

<sup>13</sup> Así lo establece el art. 28 de la Directiva. En el caso de España, es la Agencia Española de Protección de Datos (AEPD) la encargada de realizar esta función.

<sup>14</sup> Antes de iniciar estos trámites administrativos y judiciales, Max Schrems había enviado en 2011 una petición a Facebook para que le enviara todos los datos que había ido almacenando sobre él desde que comenzó a ser usuario en 2008. Recibió un CD con más de 1.200 páginas de información personal. La mayoría de los datos no supusieron una gran sorpresa, puesto que eran públicos en su perfil. No obstante, el asombro de Schrems se agravó cuando pudo comprobar que Facebook había conservado incluso la información que él había eliminado, incluidas conversaciones privadas. Es entonces cuando el Sr. Schrems inició una campaña a favor del derecho a la privacidad en la red a través de su página web: <http://europe-v-facebook.org/EN/en.html> (último acceso 29 de diciembre de 2015), donde ha ido informando hasta la fecha de todos los procedimientos administrativos y judiciales que ha iniciado.

<sup>15</sup> Así lo hace saber Maximilian Schrems en su reclamación ante el Comisario, y así lo recoge la sentencia en el apdo. 28. El propio Edward Snowden felicitaba a Schrems a través de la red social twitter el día de la publicación de la sentencia con el siguiente mensaje: «Congratulations, @MaxSchrems, you've changed the world for the better» <https://twitter.com/snowden/status/651384292728250368?lang=es> (último acceso 4 de febrero de 2016).



El Comisario desestimó la reclamación de Schrems porque consideraba que no estaba obligado a investigar sobre los hechos denunciados. Apreció que no había pruebas de que la NSA hubiera accedido a los datos personales del joven austríaco. Además, declaró que cualquier cuestión referida al carácter adecuado de la protección de los datos personales en Estados Unidos debía resolverse conforme a la Decisión en la que la Comisión Europea había constatado que Estados Unidos garantizaba un nivel adecuado de protección.

Ante esta negativa de la agencia irlandesa de protección de datos, el Sr. Schrems acudió a la vía judicial, interponiendo un recurso contra esa decisión ante la *High Court*. Este tribunal irlandés estimó que este asunto estaba dentro del ámbito de aplicación del Derecho de la Unión, en el sentido del art. 51 de la Carta de Derechos Fundamentales de la Unión Europea<sup>16</sup> (en adelante, la «Carta») por lo que la legalidad de la Decisión controvertida debía apreciarse a la luz de aquel. En esas circunstancias, la *High Court* decidió suspender el procedimiento y plantear al Tribunal de Justicia las siguientes cuestiones prejudiciales:

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 legislación 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, habida cuenta de los arts. 7, 8 y 47 de la Carta y no obstante lo dispuesto en el art. 25, apdo. 6, de la Directiva 95/46/CE?

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 vez primera la Decisión 2000/520?

#### IV. LA SENTENCIA DEL TRIBUNAL DE JUSTICIA

El Tribunal de Justicia de la Unión decide dar respuesta a las cuestiones prejudiciales elevadas por la *High Court* irlandés de forma conjunta. Con-

<sup>16</sup> Art. 51, ámbito de aplicación:

«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, estos respetarán los derechos, observarán los principios y promoverán su aplicación, con arreglo a sus respectivas competencias y dentro de los límites de las competencias que los Tratados atribuyen a la Unión».

viene destacar que las conclusiones que alcanza el Tribunal coinciden con las del abogado general Bot<sup>17</sup>, que fueron presentadas tan solo dos semanas antes de que el TJUE dictara su sentencia<sup>18</sup>. Tanto el Tribunal como el abogado general deciden sobre dos elementos cardinales: uno de tipo procedimental, relativo a los poderes de las autoridades nacionales de protección de datos y otro de tipo sustantivo, referente a la validez de la Decisión de puerto seguro.

Respecto al primer elemento, la cuestión radica en determinar si el art. 25.6 de la Directiva, entendido a la luz de los arts. 7, 8 y 47 de la Carta, debe interpretarse en el sentido de que la Decisión impide que una autoridad de control de un Estado miembro —en este asunto, el Comisario irlandés— pueda examinar la solicitud de una persona, como el Sr. Schrems, que alega que el Derecho y las prácticas en vigor en un tercer Estado —en este caso, Estados Unidos— no garantizan un nivel de protección adecuado de sus datos personales. El Tribunal realiza una argumentación que reafirma la independencia de las autoridades de control<sup>19</sup> y procede a analizar las facultades de las que estas disponen. Considera que son competentes para comprobar si una transferencia de datos personales desde el Estado miembro de esa autoridad hacia un tercer país respeta las exigencias de la Directiva<sup>20</sup>.

No obstante, el Tribunal aclara que la Decisión de la Comisión tiene carácter obligatorio para todos los Estados miembros destinatarios y vincula por tanto a todos sus órganos. Así, mientras este acto normativo no haya sido declarado inválido por el Tribunal de Justicia —que es el único competente para hacerlo<sup>21</sup>— los Estados miembros y sus órganos, entre ellos las autoridades de control como el Comisario irlandés, no pueden adoptar medidas contrarias a esa Decisión<sup>22</sup>. A pesar de ello, el Tribunal afirma que esa norma de la Comisión no puede tener el efecto de impedir que una autoridad nacional examine la solicitud de una persona que pide que se protejan sus datos personales transferidos desde un Estado miembro a un tercer país

---

<sup>17</sup> Conclusiones del abogado general Yves Bot en el asunto Schrems, C-362/14, EU:C:2015:627.

<sup>18</sup> Es importante señalar que estaba previsto que el abogado general Bot publicara sus conclusiones el 24 de junio de 2015, pero fue retrasado hasta septiembre por causas desconocidas.

<sup>19</sup> Véanse los apdos. 38 a 42 de la sentencia Schrems.

<sup>20</sup> Apdo. 47 de la sentencia Schrems.

<sup>21</sup> Apdos. 61 y 62 de la sentencia Schrems.

<sup>22</sup> Apdos. 51 y 52 de la sentencia Schrems.

al que se refiere dicha Decisión<sup>23</sup>. Por eso, aunque las autoridades nacionales no pueden declarar inválida tal acto normativo por sí mismas, cuando se encuentren ante una solicitud que impugna la compatibilidad de dicha Decisión con la protección de los derechos fundamentales, les incumbe examinar la referida solicitud «con toda la diligencia exigible»<sup>24</sup>. Aquí se abren dos posibilidades. La primera es que la autoridad llegue a la conclusión de que los datos alegados son infundados y desestime la solicitud por ello, en cuyo caso el demandante debe disponer de recursos jurisdiccionales que le permitan impugnar esa decisión ante los tribunales nacionales. La segunda es que esa autoridad considere fundadas las alegaciones y entonces debe tener capacidad para comparecer ante los tribunales nacionales, para que estos planteen al Tribunal de Justicia una cuestión prejudicial sobre la validez de la norma<sup>25</sup>. Por tanto, el TJUE falla —siguiendo la conclusión alcanzada por el abogado general Bot<sup>26</sup>— que la Decisión no impide que una autoridad de control de un Estado miembro examine la solicitud de una persona que alega que un tercer país no garantiza un nivel de protección adecuado de sus datos personales. Como consecuencia, el Comisario irlandés debe analizar la solicitud del Sr. Schrems en relación con la transferencia de sus datos a Estados Unidos. Pero, en última instancia, quien debe decidir sobre la validez del acto normativo es el Tribunal de Justicia.

A continuación, el TJUE procede a examinar el segundo aspecto fundamental de la sentencia: la validez de la Decisión de puerto seguro<sup>27</sup>. Para ello, debe apreciar si esa norma se ajusta a las exigencias derivadas de la Directiva entendida a la luz de la Carta. Según el Tribunal, el «nivel de protección adecuado» exigido por la Directiva para las transferencias de datos personales a terceros países debe entenderse en el sentido de que ese tercer país garantice un nivel de protección de derechos fundamentales «sustancialmente equiva-

---

<sup>23</sup> Apdo. 56 de la sentencia Schrems.

<sup>24</sup> Apdo. 63 de la sentencia Schrems.

<sup>25</sup> Apdo. 65 de la sentencia Schrems.

<sup>26</sup> Véase el punto 120 de las Conclusiones del abogado general Bot.

<sup>27</sup> A pesar de que el Sr. Schrems no impugnó formalmente en su recurso en el procedimiento principal la validez de la Decisión ni el tribunal irlandés lo plantea en sus cuestiones prejudiciales, como bien señala el abogado general en el punto 124 de sus conclusiones: «la apreciación de si Estados Unidos garantiza un nivel de protección adecuado de los datos de carácter personal transferidos en el marco del régimen de puerto seguro, conduce necesariamente a reflexionar sobre la validez de dicha Decisión».

lente»<sup>28</sup> al asegurado en la Unión<sup>29</sup>. Por eso, la Comisión tiene la obligación, al valorar el nivel de protección ofrecido por un tercer país, de apreciar el contenido de las reglas aplicables en él, así como la práctica seguida para asegurar su cumplimiento<sup>30</sup>.

El Tribunal pone de manifiesto que la Decisión de la Comisión reconoce la primacía de las «exigencias de seguridad nacional, interés público y cumplimiento de la ley (de Estados Unidos)» sobre los principios de puerto seguro. Consecuentemente, las entidades estadounidenses autocertificadas que reciban datos personales desde la Unión están obligadas a dejar de aplicar esos principios cuando estos entren en conflicto con esas exigencias<sup>31</sup>. Así, la Decisión permite injerencias en los derechos fundamentales de las personas cuyos datos personales se transfieren desde la Unión a Estados Unidos. Es en este punto donde el Tribunal identifica dos fallas de la Decisión en relación con la legislación estadounidense. En primer lugar, esa norma no contiene ninguna constatación sobre la existencia de reglas en ese país destinadas a limitar las posibles intrusiones en los derechos fundamentales de las personas cuyos datos se transfieran desde la Unión a Estados Unidos. En segundo lugar, la Decisión no pone de manifiesto la existencia de una protección jurídica eficaz contra injerencias de esa naturaleza, es decir, los ciudadanos no disponen de vías jurídicas en Estados Unidos que les permitan acceder a los datos que les pertenecen y conseguir, en su caso, su rectificación o supresión<sup>32</sup>. Por con-

---

<sup>28</sup> Al emplear esta expresión, el TJUE parece inspirarse en dos casos paradigmáticos tanto a nivel nacional como europeo. En primer lugar, en la archifamosa sentencia «*Solange II*» de 22 de octubre de 1986 (BVerfGE 73, 339 2 BvR 197/83), en la que el Tribunal Constitucional alemán (*Bundesverfassungsgericht*) declaró que no revisaría la compatibilidad del Derecho Comunitario con los derechos fundamentales de la Constitución alemana siempre que la Unión Europea y, en particular, el Tribunal de Luxemburgo, garantizaran una protección de los derechos en un grado «esencialmente equivalente». En segundo lugar, en la emblemática sentencia del Tribunal Europeo de Derechos Humanos *Bosphorus* núm. 45036/98, de 30 de junio de 2005, donde el Tribunal declaró que la acción de un Estado para dar cumplimiento a sus obligaciones internacionales estaría justificada en tanto en cuanto esa organización internacional protegiera los derechos fundamentales de una forma al menos «equivalente» a la exigida por el Convenio Europeo de Derechos Humanos.

<sup>29</sup> Apdos. 73 y 74 de la sentencia Schrems.

<sup>30</sup> Apdo. 75 de la sentencia Schrems.

<sup>31</sup> Apdo. 86 de la sentencia Schrems.

<sup>32</sup> Es relevante señalar, como indica el Tribunal en el apdo. 90 de la sentencia, que este examen de la Decisión es confirmado por la apreciación que la misma Comisión realizó, a raíz de la polémica desatada por las revelaciones de Snowden, en dos documentos

siguiente, el TJUE considera que una normativa como la estadounidense que permite a las autoridades públicas acceder de forma generalizada al contenido de las comunicaciones electrónicas vulnera el contenido esencial del derecho fundamental al respeto de la vida privada garantizado por el art. 7 de la Carta<sup>33</sup>. De igual forma, una normativa que no prevé posibilidad alguna de que el ciudadano ejerza acciones jurídicas para acceder a los datos personales que le conciernen o para obtener su rectificación o supresión no respeta el contenido esencial del derecho fundamental a la tutela judicial efectiva reconocido en el art. 47 de la Carta<sup>34</sup>.

Por estas razones, el Tribunal declara que la Comisión no manifestó en la Decisión que Estados Unidos garantizara efectivamente un nivel de protección adecuado<sup>35</sup>. Consecuentemente, el Tribunal concluye que el art. 1 de la Decisión vulnera las exigencias establecidas por el art. 25.6 de la Directiva,

---

de 27 de noviembre de 2013: la Comunicación al Parlamento Europeo y al Consejo titulada «Restablecer la confianza en los flujos de datos entre la UE y EE.UU.» («COM(2013) 846 final») y la Comunicación al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE («COM(2013) 847 final»). En ambas comunicaciones, el ejecutivo de la Unión constató que las autoridades estadounidenses podían acceder a los datos personales transferidos a su territorio y tratarlos de manera incompatible con las finalidades de ese traspaso, que iba más allá de lo que era estrictamente necesario y proporcionado para la protección de la seguridad nacional. Asimismo, la Comisión apreció que las personas afectadas no disponían de vías jurídicas administrativas o judiciales que les permitieran acceder a los datos que les concernían y obtener, en su caso, su rectificación o supresión.

<sup>33</sup> Apdo. 94 de la sentencia Schrems.

<sup>34</sup> Apdo. 95 de la sentencia Schrems.

<sup>35</sup> Apdo. 97 de la sentencia Schrems. Interesa señalar que el abogado general Bot es mucho más duro con la «omisión» de la Comisión en su deber de comprobar que el tercer país garantizaba un nivel adecuado de protección. El abogado general considera que la Comisión debería haber suspendido la Decisión de puerto seguro. Véanse los puntos 217 a 236 de sus conclusiones. Conviene subrayar el punto 234 respecto a la responsabilidad de la Comisión: «si bien tenía conocimiento de la existencia de disfunciones en la aplicación de la Decisión 2000/520, la Comisión ni la suspendió ni la adaptó, lo que dio lugar a la violación continuada de los derechos fundamentales de las personas cuyos datos de carácter personal fueron y siguen siendo transferidos en el marco del régimen de puerto seguro». Asimismo, cobra indudable importancia el punto 236: «Tal inacción de la Comisión, que atenta directamente contra los derechos fundamentales protegidos por los arts. 7, 8 y 47 de la Carta, constituye, a mi parecer, un motivo complementario para declarar inválida la Decisión 2000/520 en el marco de la presente remisión prejudicial».

entendido a la luz de la Carta, y es inválido por esa causa<sup>36</sup>. Igualmente, el Tribunal considera inválido el art. 3.1 de la Decisión, puesto que priva a las autoridades nacionales de las facultades que les atribuye el art. 28 de la Directiva, en el supuesto de que una persona alegue factores que puedan afectar a la validez de una Decisión de la Comisión como la controvertida<sup>37</sup>. Según el Tribunal, los arts. 1 y 3 de esta norma son indisociables de los arts. 2 y 4 y de los anexos de esta, por lo que declara que toda la Decisión en su conjunto es inválida<sup>38</sup>.

## V. VALORACIÓN DE LA SENTENCIA

### 1. SOBRE LA INDEPENDENCIA DE LAS AUTORIDADES NACIONALES DE PROTECCIÓN DE DATOS

La decisión en el caso Schrems se inserta plenamente en la línea jurisprudencial del Tribunal que blinda la independencia de las autoridades nacionales de protección de datos. En efecto, en tres sentencias anteriores, el Tribunal consideró que Alemania, Austria y Hungría habían violado la Directiva precisamente porque no habían respetado la «completa independencia» que esta norma prescribe respecto de las autoridades. Alemania fue condenada porque sus parlamentos podían ejercer demasiado control sobre su autoridad nacional<sup>39</sup>. Por su parte, el incumplimiento de Austria se debía a que no había separado correctamente su autoridad de protección de datos del funcionamiento ordinario<sup>40</sup>. En el caso de Hungría, inobservó la Directiva al defenestrar al dirigente de su agencia de control antes de que el período para el cual había

<sup>36</sup> Apdos. 97 y 98 de la sentencia.

<sup>37</sup> Apdos. 99-104 de la sentencia.

<sup>38</sup> A pesar de que tanto el Tribunal como el abogado general alcanzan la conclusión de que la Decisión es inválida, conviene destacar las diferencias en su aproximación. La razón que da el Tribunal para considerarla nula pivota en torno al art. 25.6 de la Directiva, mientras el abogado general pone mucho más énfasis en la vulneración de derechos fundamentales, como puede leerse en el punto 216: «procede declarar la nulidad de dicha Decisión en la medida en que, habida cuenta de las violaciones de los derechos fundamentales anteriormente descritos, no cabe considerar que el régimen de puerto seguro por ella instaurado garantiza un nivel de protección adecuado de los datos de carácter personal transferidos desde la Unión a Estados Unidos con arreglo a dicho régimen».

<sup>39</sup> Sentencia del Tribunal de Justicia Comisión/Alemania, C-518/07, EU:C:2010:125.

<sup>40</sup> Sentencia del Tribunal de Justicia Comisión/Austria, C 614/10, EU:C:2012:631.

sido nombrado expirara<sup>41</sup>. Asimismo, en la sentencia en el asunto Weltimmo<sup>42</sup>, dictada tan solo cinco días antes que el fallo judicial en el caso Schrems —aunque con mucha menor popularidad que esta<sup>43</sup>—, el Tribunal reconocía aún mayor poder a las autoridades nacionales, declarando que estas podían tener competencia incluso más allá de sus fronteras, sobre entidades registradas en otro Estado miembro, siempre que ejercieran una actividad efectiva y real en el territorio del Estado de esa autoridad de control<sup>44</sup>. Hay autores que apuntan a que es precisamente la combinación de ambas sentencias —Schrems y Weltimmo— lo que indica que el Tribunal prioriza una protección de datos descentralizada sobre la uniformidad<sup>45</sup>.

Así, resulta paradójico que el Tribunal declare, por un lado, en línea con su consolidada jurisprudencia iniciada en el caso Foto-Frost<sup>46</sup>, que es el único competente para declarar la invalidez de un acto de la Unión apoyándose en la necesidad de salvaguardar la seguridad jurídica<sup>47</sup> y, por otro, permita que las agencias nacionales de protección de datos puedan suspender las transferencias de datos de forma unilateral<sup>48</sup>. Parece que es difícil reconciliar la inde-

<sup>41</sup> Sentencia del Tribunal de Justicia Comisión/Hungría, C288/12 EU:C:2014:237.

<sup>42</sup> Sentencia del Tribunal de Justicia Weltimmo, C-230/14, EU:C:2015:639.

<sup>43</sup> Es interesante el artículo de Denis Kelleher, escrito con anterioridad a la publicación de la sentencia, que advierte de la importancia del caso Weltimmo, que ha pasado desapercibido a la sombra de Schrems, con un título revelador: «You're Watching Schrems, but Maybe You Should Be Watching Weltimmo» <https://iapp.org/news/a/cjeu-case-to-determine-who-can-regulate-whom/> (último acceso 8 de enero de 2016).

<sup>44</sup> Véase un análisis de las sentencia Schrems y Weltimmo en Pedro A. DE MIGUEL ASENSIO, «Aspectos internacionales de la protección de datos: las sentencias Schrems y Weltimmo del Tribunal de Justicia», *La Ley Unión Europea*, núm. 31, 2015, pp. 1-10. Sobre la sentencia Weltimmo, véase también el comentario de Lorna Woods, en el blog EU law analysis, de 13 de octubre de 2015, <http://eulawanalysis.blogspot.com.es/2015/10/data-protection-cjeu-clarifies.html> (último acceso 8 de enero de 2016).

<sup>45</sup> Christina ECKES y Vigjilencia ABAZI, «Safe Harbour Case: Safeguarding European Fundamental Rights or Creating a Patchwork of National Data Protection?», *UK Constitutional Law Blog*, 9 de octubre de 2015, disponible en: <http://ukconstitutionallaw.org/2015/10/09/christina-eckes-and-vigjilencia-abazi-safe-harbour-case-safeguarding-european-fundamental-rights-or-creating-a-patchwork-of-national-data-protection/> (último acceso 8 de enero de 2016).

<sup>46</sup> Sentencia del Tribunal de Justicia Foto-Frost, C-314/85, EU:C:1987:452.

<sup>47</sup> Véanse los apdos. 61 y 62 de la sentencia Schrems.

<sup>48</sup> Orla LINSKEY, «Negotiating the Data Protection Thicket: Life in the Aftermath of Schrems», *Verfassungsblog*, 9 de octubre de 2015 disponible en: <http://verfassungsblog.de/negotiating-the-data-protection-thicket-life-in-the-aftermath-of-schrems/> (último acceso 14 de enero de 2016).

pendencia que el Tribunal otorga a las agencias nacionales de protección de datos con su insistencia en la seguridad jurídica y la aplicación uniforme del Derecho de la Unión en los 28 Estados miembros. Por tanto, este pronunciamiento abre la puerta a un complicado entramado de decisiones de multitud de autoridades sobre si los datos de una empresa determinada pueden ser transmitidos o no en cada caso individual, en detrimento de la uniformidad en la aplicación del Derecho de la Unión<sup>49</sup>.

En suma, este fallo judicial refuerza aún más la independencia de las autoridades nacionales —«los superhéroes del mundo de la protección de datos»<sup>50</sup>—, que serán capaces de evaluar cada petición en relación a las transferencias internacionales de datos y podrán suspenderlas en caso de que consideren que vulnera la legislación. Lo que no podrán hacer, como ninguna otra autoridad nacional administrativa o judicial, es declarar la invalidez de un acto normativo comunitario, para lo cual es única y exclusivamente competente el Tribunal de la Unión —cuestión que no es novedosa, sino que conocemos desde su jurisprudencia de los años ochenta—.

## 2. LA DECLARACIÓN DE INVALIDEZ DE LA DECISIÓN Y LA VULNERACIÓN DE DERECHOS FUNDAMENTALES

No todos los días se lee una sentencia en la que el Tribunal invalida un acto normativo de la Unión porque lesiona el «contenido esencial»<sup>51</sup> de derechos fundamentales consagrados en la Carta —más concretamente, los arts. 7 y 47<sup>52</sup>—. En este sentido, Schrems marca un hito en la jurisprudencia

<sup>49</sup> Christina ECKES y Vigjilencia ABAZI, *op. cit.*, p. 2.

<sup>50</sup> Steve PEERS, «When super-regulators fight: the ‘one-stop shop’ in the proposed Data Protection Regulation», *EU Law Analysis blog*, 11 marzo de 2015 <http://eulawanalysis.blogspot.com.es/2015/03/when-super-regulators-fight-one-stop.html> (último acceso 14 de enero de 2016)

<sup>51</sup> Véanse los apdos. 94 y 95 de la sentencia Schrems.

<sup>52</sup> Interesa señalar que el Tribunal tuvo en cuenta el derecho a la protección de los datos de carácter personal (art. 8 de la Carta) para la primera parte de su decisión (sobre si las autoridades nacionales podían separarse o no de la Decisión de la Comisión), así como para declarar inválido el art. 3 de la Decisión, pero consideró que esta tan solo vulneraba el «contenido esencial» del derecho a la privacidad (art. 7) y el derecho a la tutela judicial efectiva (art. 47), sin hacer referencia al art. 8. La diferencia entre el derecho a la privacidad y el derecho a la protección de los datos de carácter personal es compleja, ya que el último surgió como derivado del primero en la jurisprudencia hasta convertirse en derecho autónomo. Sobre el tratamiento que los tribunales de Luxemburgo y Estrasburgo han realizado de estos derechos, véase Julianne KOKOTT



europea de defensa de los derechos fundamentales y de forma más concreta, del derecho a la privacidad. Por eso, debe analizarse en el contexto más global en el que se enmarca, en un debate continuo entre seguridad pública, intereses comerciales y libertades de los ciudadanos. Así, no podemos olvidar dos casos emblemáticos en este ámbito: Digital Rights Ireland<sup>53</sup> —en el que el Tribunal anuló la Directiva 2006/24/CE sobre conservación de datos en relación con las comunicaciones electrónicas<sup>54</sup>— y Google Spain<sup>55</sup> —donde se consagró el denominado «derecho al olvido» de los ciudadanos sobre el interés económico del gestor del motor de búsqueda.

Una de las críticas que la sentencia Schrems ha recibido es, precisamente, en referencia a la declaración de invalidez de la Decisión, ya que, a diferencia del caso Digital Rights Ireland<sup>56</sup>, el tribunal remitente no cuestionaba la validez del acto normativo. Por esa razón, hay autores que consideran que el Tribunal podría haber respondido a las cuestiones preliminares de la *High Court* irlandesa sin necesidad de pronunciarse sobre la validez de la Decisión<sup>57</sup>. Lo cierto es que el TJUE creyó que era necesario decidir sobre esa cuestión<sup>58</sup>,

---

y Christoph SOBOTTA, «The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR», *International Data Privacy Law*, 2013, vol. 3, núm. 4, pp. 222 y ss.

<sup>53</sup> Sentencia del Tribunal de Justicia de la Unión Digital Rights Ireland, asuntos acumulados C-293/12 y C-594/12, EU:C:2014:238. Para un análisis de esta sentencia y de la posición de los tribunales nacionales frente a la Directiva de retención de datos, véase Maribel GONZÁLEZ PASCUAL, «El TJUE como garante de los derechos en la UE a la luz de la sentencia Digital Rights Ireland» *Revista de Derecho Comunitario Europeo* núm. 49, 2014, pp. 943-971.

<sup>54</sup> Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE (DO L 105, de 13 de abril de 2006, p. 54).

<sup>55</sup> Sentencia del Tribunal de Justicia de la Unión Google Spain, C 131/12, EU:C:2014:317. Véase Indra DÖHMANN, «A new framework for information markets: *Google Spain*», *Common Market Law Review*, 52: pp. 1033-1058.

<sup>56</sup> Es importante señalar que Digital Rights Ireland intervino en el procedimiento del asunto Schrems ante el Tribunal de Justicia de la Unión, lo cual da buena cuenta de la estrecha relación entre ambas sentencias.

<sup>57</sup> Christina ECKES y Vigilenca ABAZI, *op. cit.*, p. 2.

<sup>58</sup> El Tribunal justifica la necesidad de apreciar la validez de la Decisión en el apdo. 67 de la sentencia: «Según resulta de las explicaciones del tribunal remitente sobre las cuestiones planteadas, en el asunto principal el Sr. Schrems alega que el Derecho y las prácticas de Estados Unidos no garantizan un nivel de protección adecuado, en el

convirtiendo al caso Schrems en un pronunciamiento altamente significativo respecto a la jurisprudencia anterior por dos razones. Por primera vez, el TJUE consideró que la injerencia del acto normativo no respetaba el contenido esencial del derecho a la privacidad<sup>59</sup>. En segundo lugar, al identificar que la intrusión no respetaba la esencia de ese derecho, no fue necesario llevar a cabo un análisis de proporcionalidad a la luz del art. 52.1 de la Carta<sup>60</sup>, como sí se realizó, en cambio, en *Digital Rights Ireland*<sup>61</sup>, donde la invalidez de la Directiva se basó fundamentalmente en el resultado de este test<sup>62</sup>. De esta forma, *Digital Rights Ireland* abrió el camino y el Tribunal ha avanzado por el mismo en el caso Schrems<sup>63</sup>.

Asimismo, esta sentencia tiene importantes implicaciones para la tutela multinivel de los derechos fundamentales en Europa, tanto en lo referente a la relación del Derecho de la Unión con los ordenamientos jurídicos nacionales como a la relación de aquel con el Convenio Europeo para la Protección de los Derechos Humanos y las Libertades Fundamentales («CEDH»), y su mecanismo de control, el Tribunal Europeo de Derechos Humanos (TEDH).

---

sentido del art. 25 de la Directiva 95/46. Como ha señalado el abogado general en los puntos 123 y 124 de sus conclusiones, el Sr. Schrems manifiesta dudas, que ese tribunal parece compartir en sustancia, sobre la validez de la Decisión 2000/520. Siendo así, por las consideraciones expuestas en los apdos. 60 a 63 de la presente sentencia, y para dar una respuesta completa al referido tribunal, es preciso apreciar si esa Decisión se ajusta a las exigencias derivadas de dicha Directiva entendida a la luz de la Carta».

<sup>59</sup> Así lo reconoce el propio Herwig Hofmann, abogado de Maximilian Schrems en este caso, en el comentario a la sentencia que realiza en <http://europaeuslaw.blogspot.nl/2015/11/herwig-hofmann-on-schrems-decision.html> (último acceso 8 de enero de 2016).

<sup>60</sup> Art. 52.1 de la Carta: «Cualquier limitación del ejercicio de los derechos y libertades reconocidos por la presente Carta deberá ser establecida por la ley y respetar el contenido esencial de dichos derechos y libertades. Dentro del respeto del principio de proporcionalidad, solo podrán introducirse limitaciones cuando sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás».

<sup>61</sup> Véanse los apdos. 45 a 69 de la sentencia *Digital Rights Ireland*.

<sup>62</sup> Apdo. 69 de la sentencia *Digital Rights Ireland*: «Habida cuenta de todas las consideraciones anteriores, ha de considerarse que, al adoptar la Directiva 2006/24, el legislador de la Unión sobrepasó los límites que exige el respeto del principio de proporcionalidad en relación con los arts. 7, 8 y 52, apdo. 1, de la Carta».

<sup>63</sup> Martin SCHEININ, «The Essence of Privacy, and Varying Degrees of Intrusion», *Verfassungsblog*, 7 de octubre de 2015, disponible en: <http://verfassungsblog.de/the-essence-of-privacy-and-varying-degrees-of-intrusion/> (último acceso 26 de diciembre de 2015).

En cuanto al primer caso, si la sentencia Schrems afirma sin fisuras que la legislación de Estados Unidos no protege de una forma «sustancialmente equivalente» los derechos fundamentales de los europeos, también debemos plantearnos hasta qué punto los sistemas nacionales lo hacen. A este respecto, es conveniente tener en cuenta que las revelaciones de Snowden pusieron de manifiesto las semejanzas entre el programa de vigilancia estadounidense *Prism* y el sistema británico *Tempora*<sup>64</sup>. De hecho, un mes después de la publicación de la sentencia Schrems, un tribunal británico decidió elevar una cuestión prejudicial al TJUE sobre la compatibilidad de la *Data Retention and Investigatory Powers Act* («DRIPA») de 2014 con el Derecho de la Unión<sup>65</sup>.

En lo referente al segundo ámbito, es muy sorprendente que en un caso como Schrems, donde los derechos fundamentales juegan un papel esencial, el Tribunal de Luxemburgo no cite en absoluto el CEDH ni la jurisprudencia del Tribunal de Estrasburgo<sup>66</sup>. Así se confirma la tendencia de «autonomización» del TJUE respecto del TEDH —del que varios autores alertan<sup>67</sup>— tras la entrada en vigor del Tratado de Lisboa en 2009, cuando la Carta comenzó a ser jurídicamente vinculante. En este sentido, conviene hacer referencia a la

<sup>64</sup> Orla LINSKEY, *op. cit.*, p. 1.

<sup>65</sup> Véanse las cuestiones prejudiciales planteadas por el tribunal británico en: <https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/11/Davis-FINAL.pdf> (último acceso 27 de diciembre de 2015). Este caso ha sido registrado en el Tribunal de Justicia de la Unión el 28 de diciembre de 2015 con el número de asunto C-698/15 Davis and Others. Véase un comentario sobre los antecedentes de este caso en «Case C-698/15, Davis – did the CJEU in Digital Rights Ireland intend to lay down mandatory requirements of EU law?» *EU law radar*, <http://eulawradar.com/case-c-69815-davis-did-the-cjeu-in-digital-rights-ireland-intend-to-lay-down-mandatory-requirements-of-eu-law/> (último acceso 2 de febrero de 2016).

<sup>66</sup> Teniendo en consideración que el art. 7 de la Carta es coincidente con el art. 8 del CEDH y que el art. 52.3 de la Carta establece lo siguiente: «En la medida en que la presente Carta contenga derechos que correspondan a derechos garantizados por el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, su sentido y alcance serán iguales a los que les confiere dicho Convenio (...)».

<sup>67</sup> Johan CALLEWAERT, «To accede or not to accede: European protection of fundamental rights at the crossroads», *Journal Européen des droits de l'homme*, 2014, p. 500 y ss.; Grainne DE BURCA, «After the EU Charter of Fundamental Rights: the Court of Justice as a Human Rights Adjudicator? *Maastricht Journal of European and Comparative Law*, 2013, p. 174.

reciente sentencia del Tribunal de Estrasburgo en el asunto *Zakharov*<sup>68</sup> donde condena a Rusia porque su sistema de interceptación de las comunicaciones vulnera el art. 8 del Convenio<sup>69</sup>. A diferencia del TJUE, el TEDH sí se hace eco de la jurisprudencia de aquel en materia de protección del derecho al respeto de la vida privada, particularmente, de la sentencia *Digital Rights Ireland*<sup>70</sup>. Asimismo, en enero de 2016, el Tribunal de Estrasburgo ha condenado a Hungría por violación del art. 8 del CEDH en el asunto también relativo a la vigilancia masiva *Szabó and Vissy v. Hungary*<sup>71</sup>, donde hace referencia a la jurisprudencia del Tribunal de Luxemburgo, más concretamente, a las sentencias *Digital Rights Ireland* y *Schrems*<sup>72</sup>. En el mismo mes, el TEDH también ha dictado sentencia en otro caso referente al art. 8 del Convenio, *Barbulescu v. Romania*<sup>73</sup>, en el que se hace eco de la normativa de la Unión Europea en materia de derecho a la privacidad y protección de datos<sup>74</sup>, aunque no de la jurisprudencia del TJUE<sup>75</sup>.

Además, este pronunciamiento supone la afirmación del Tribunal de Justicia como garante del estándar de protección de derechos fundamentales por parte de la Unión Europea en el orden internacional<sup>76</sup>, siguiendo la senda de la

<sup>68</sup> Sentencia del Tribunal Europeo de Derechos Humanos (Gran Sala) de 5 de diciembre de 2015, *Roman Zakharov c. Rusia*, núm. solicitud 47143/06. Véase un comentario a esta sentencia de Lorna WOODS, «L. Zakharov v Russia: Mass Surveillance and the European Court of Human Rights», de 16 de diciembre de 2015, *EU Law Analysis Blog*, [http://eulawanalysis.blogspot.com.es/2015/12/zakharov-v-russia-mass-surveillance-and.html?utm\\_source=feedburner&utm\\_medium=email&utm\\_campaign=Feed:+EuLawAnalysis+\(EU+Law+Analysis\)](http://eulawanalysis.blogspot.com.es/2015/12/zakharov-v-russia-mass-surveillance-and.html?utm_source=feedburner&utm_medium=email&utm_campaign=Feed:+EuLawAnalysis+(EU+Law+Analysis)) (último acceso 27 de diciembre de 2015).

<sup>69</sup> El art. 8 del CEDH recoge el derecho al respeto a la vida privada y familiar.

<sup>70</sup> Véase el apdo. 147 de la sentencia *Zakharov*.

<sup>71</sup> Sentencia del Tribunal Europeo de Derechos Humanos de 12 de enero de 2016, *Szabó and Vissy v. Hungary*, núm. de solicitud 37138/14.

<sup>72</sup> Véanse los apdos. 15 y 23 de la sentencia *Szabó*.

<sup>73</sup> Sentencia del Tribunal Europeo de Derechos Humanos de 12 de enero de 2016, *Barbulescu v. Romania*, núm. de solicitud 61496/08. Puede verse un comentario a esta sentencia en Steve PEERS, «Is Workplace Privacy Dead? Comments on the Barbulescu judgment», *EU law analysis blog*, 14 de enero de 2016, disponible en: [http://eulawanalysis.blogspot.com.es/2016/01/is-workplace-privacy-dead-comments-on.html?utm\\_source=feedburner&utm\\_medium=email&utm\\_campaign=Feed:+EuLawAnalysis+\(EU+Law+Analysis\)](http://eulawanalysis.blogspot.com.es/2016/01/is-workplace-privacy-dead-comments-on.html?utm_source=feedburner&utm_medium=email&utm_campaign=Feed:+EuLawAnalysis+(EU+Law+Analysis)) (último acceso 15 de enero de 2016).

<sup>74</sup> Véase el apdo. 18 de la sentencia *Barbulescu*.

<sup>75</sup> En cambio, sí la cita el juez Pinto de Albuquerque en su voto particular, concretamente, en el pie de página 10.

<sup>76</sup> ECKES, C. y ABAZI, V. *op. cit.*

emblemática sentencia *Kadi*<sup>77</sup>. No obstante, Luxemburgo aplica un estándar de protección mayor de los derechos cuando se enfrenta a actos normativos de la propia Unión que cuando se trata de actos nacionales que entran dentro del ámbito de aplicación de la Carta. En efecto, podemos observar que, en el segundo tipo de casos, como, por ejemplo, *Delvigne*<sup>78</sup> o *Celaj*<sup>79</sup>, concernientes a actos nacionales, el Tribunal aplica el estándar de protección mínimo. En cambio, cuando se trata de actos de la propia Unión, como en los asuntos *Schecke*<sup>80</sup>, *Test Achats*<sup>81</sup>, *Digital Rights Ireland* y el mismo *Schrems*, el Tribunal ha puesto de manifiesto un alto grado de escrutinio del respeto de los derechos fundamentales<sup>82</sup>. En este sentido, está pendiente la resolución del Dictamen 1/15 donde el Tribunal deberá decidir sobre dos cuestiones relativas al Acuerdo entre Canadá y la Unión Europea sobre el tratamiento y la transferencia de datos del registro de nombres de los pasajeros: si la base jurídica elegida es la adecuada y si es compatible con los arts. 7, 8 y 52. 1 de la Carta de Derechos Fundamentales de la Unión<sup>83</sup>. La sentencia *Schrems* constituye un importante

<sup>77</sup> Sentencia del Tribunal de Justicia C-402/05 P y C-415/05 P *Kadi y Al Barakaat* EU:C:2008:461. Aunque los hechos eran absolutamente diferentes, y salvando las distancias entre ambos casos, *Schrems* puede asemejarse a *Kadi* en el sentido de que el Tribunal afirmó su capacidad para revisar la validez de un acto normativo a la luz del estándar de protección de derechos fundamentales de la Unión Europea.

<sup>78</sup> Sentencia del Tribunal de Justicia C-650/13 *Delvigne* EU:C:2015:648.

<sup>79</sup> Sentencia del Tribunal de Justicia C-290/14 *Celaj* EU:C:2015:640.

<sup>80</sup> Sentencia del Tribunal de Justicia C-92/09 *Volker*, EU:C:2010:662. En esta sentencia, por primera vez, el TJUE anuló legislación secundaria (concretamente, varios artículos del Reglamento núm. 1290/2005) sobre la base de la Carta.

<sup>81</sup> Sentencia del Tribunal de Justicia (Gran Sala) C-236/09 *Test-Achats*, EU:C:2011:100. El Tribunal declaró inválido el art. 5, apdo. 2, de la Directiva 2004/113/CE por ser incompatible con los arts. 21 y 23 de la Carta.

<sup>82</sup> Daniel SARMIENTO, «What *Schrems*, *Delvigne* and *Celaj* tell us about the state of fundamental rights in the EU», 16 de octubre de 2015, *Despite our differences Blog*, <https://despiteourdifferencesblog.wordpress.com/2015/10/16/what-schrems-delvigne-and-celaj-tell-us-about-the-state-of-fundamental-rights-in-the-eu/> (último acceso 27 de diciembre de 2015).

<sup>83</sup> Este dictamen ha sido solicitado por el Parlamento Europeo, sobre la base del art. 218.11 del TFUE. Pueden consultarse las preguntas que se plantean al Tribunal en: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=163590&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=215996> (último acceso 2 de febrero de 2016). Véase la Resolución del Parlamento Europeo sobre la solicitud de un dictamen al TJUE: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2014-0058+0+DOC+XML+V0//ES> (último acceso 3 de febrero de 2016).

precedente y se espera, por tanto, que tenga una importante influencia sobre ese pronunciamiento.

Por último, es inevitable cuestionarse qué régimen gobernará las transferencias de datos entre la Unión Europea y los Estados Unidos una vez anulada la decisión de puerto seguro. Tras la publicación de la sentencia Schrems, la Comisión Europea aprobó una comunicación indicando las vías alternativas para la transmisión de datos entre ambas orillas del Atlántico e intensificó las negociaciones con Estados Unidos para lograr un nuevo acuerdo<sup>84</sup>. El Grupo de Trabajo del art. 29 —órgano consultivo independiente creado por la Directiva e integrado por las autoridades de Protección de Datos de todos los Estados miembros, el Supervisor Europeo de Protección de Datos y la Comisión Europea<sup>85</sup>— instó a las instituciones europeas y a los Estados a iniciar urgentemente negociaciones con Estados Unidos para conseguir una solución antes del 31 de enero de 2016<sup>86</sup>. Justo después del término de ese plazo, el 2 de febrero, la Comisión Europea anunció que había alcanzado un acuerdo con Estados Unidos para establecer un nuevo marco normativo: el *EU-US Privacy Shield* (escudo de privacidad)<sup>87</sup>.

El nuevo acuerdo incluye una serie de salvaguardias para cumplir con las exigencias establecidas por el Tribunal en Schrems. Según el comunicado de la Comisión, por primera vez Estados Unidos se ha comprometido por escrito a asegurar que el acceso a los datos de los ciudadanos europeos por parte de sus autoridades estará sujeto a claras limitaciones y mecanismos de vigilancia. Además, habrá una revisión anual de este acuerdo por parte de la Comisión Europea y del Departamento de Comercio de Estados Unidos, con la participación de expertos tanto de las autoridades nacionales europeas

---

<sup>84</sup> Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems) [http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-us\\_data\\_flows\\_communication\\_final.pdf](http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-us_data_flows_communication_final.pdf) (último acceso 3 de febrero de 2016).

<sup>85</sup> Para más información sobre su composición, estructura y normas de procedimiento, véase: [http://ec.europa.eu/justice/data-protection/article-29/index\\_en.htm](http://ec.europa.eu/justice/data-protection/article-29/index_en.htm) (último acceso 3 de febrero de 2016).

<sup>86</sup> Véase la Declaración del Grupo de Trabajo de art. 29 de 16 de octubre de 2015 [http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29\\_press\\_material/2015/20151016\\_wp29\\_statement\\_on\\_schrems\\_judgement.pdf](http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf) (último acceso 3 de febrero de 2016).

<sup>87</sup> Véase la nota de prensa de la Comisión Europea [http://europa.eu/rapid/press-release\\_IP-16-216\\_en.htm?locale=en](http://europa.eu/rapid/press-release_IP-16-216_en.htm?locale=en) (último acceso 3 de febrero de 2016).

como estadounidenses. Asimismo, se garantiza que los ciudadanos tengan garantizada una tutela judicial efectiva en lo referente a sus datos, abriendo la vía a que las autoridades nacionales europeas puedan remitir las reclamaciones al Departamento de Comercio estadounidense y creando la figura del Defensor del Usuario («Ombudsperson»). Sin embargo, hay autores que consideran que, mientras la legislación estadounidense adolezca de las mismas fallas que el Tribunal ha identificado en Schrems, ningún acuerdo «*Safe Harbour 2.0.*» podrá respetar las exigencias de protección de los derechos fundamentales de la Unión Europea<sup>88</sup>. Veremos cómo se concreta el acuerdo en la legislación<sup>89</sup>. En caso de que el Tribunal deba pronunciarse sobre su validez como sucedió con la Decisión puerto seguro, comprobaremos si el *Privacy Shield* sobrevive o no al examen de Luxemburgo<sup>90</sup>. Esperamos que el Tribunal mantenga el alto grado de escrutinio de defensa de los derechos fundamentales que ha manifestado en Schrems.

## VI. CONSIDERACIONES FINALES

La sentencia en el caso Schrems tiene importantísimas implicaciones. Por un lado, de carácter teórico, ya que supone una contribución esencial para la comprensión de la estructura y los efectos jurídicos de los derechos fundamentales recogidos en la Carta, más concretamente, para la interpretación del derecho al respeto de la vida privada (art. 7), la protección de los datos de carácter personal (art. 8) y la tutela judicial efectiva (art. 47). En este sentido, aporta un parámetro de medida esencial para analizar el respeto de las libertades individuales por parte de los sistemas de vigilancia masiva (tanto de terceros Estados como de los propios Estados miembros). Por otro lado, sus

---

<sup>88</sup> Paul BERNAL, «The Surveillance Elephant in the Room...», 7 de octubre de 2015, Paul bernal's Blog, <https://paulbernal.wordpress.com/2015/10/07/the-surveillance-elephant-in-the-room/> (último acceso 3 de febrero de 2016); Orla LINSKEY, *op. cit.*, p. 1.

<sup>89</sup> En el momento de entrega del presente comentario, ni siquiera el acuerdo se ha hecho público. Tan solo conocemos su contenido a través del comunicado de prensa de la Comisión.

<sup>90</sup> Steve Peers se muestra escéptico hacia el nuevo acuerdo y considera probable que este sea impugnado ante el Tribunal de Justicia de la Unión dentro de poco tiempo. Véase Steve PEERS, «Live. Die. Repeat. The 'Privacy Shield' deal as 'Groundhog Day': endlessly making the same mistakes?», EU Law Analysis, 3 de febrero de 2016, [http://eulawanalysis.blogspot.it/2016/02/live-die-repeat-privacy-shield-deal-as.html?utm\\_source=feedburner&utm\\_medium=email&utm\\_campaign=Feed:+EuLawAnalysis+\(EU+Law+Analysis\)](http://eulawanalysis.blogspot.it/2016/02/live-die-repeat-privacy-shield-deal-as.html?utm_source=feedburner&utm_medium=email&utm_campaign=Feed:+EuLawAnalysis+(EU+Law+Analysis)) (último acceso 3 de febrero de 2016).

consecuencias prácticas son innegables: en primer lugar y de un modo muy directo, para las entidades que estaban adheridas a los principios de puerto seguro y, en segundo lugar, para las relaciones de la Unión con los Estados Unidos, sobre todo, en un momento delicado en el que el Tratado de Asociación Transatlántica de Comercio e Inversión (más conocido por sus siglas en inglés «TTIP») está aún en proceso de negociación.

Asimismo, esta sentencia tiene una amplia repercusión en términos de legitimidad de las instituciones. El Tribunal de Justicia sale reforzado al erigirse como el máximo garante de los derechos fundamentales de los ciudadanos europeos y al trazar unas líneas rojas muy determinadas que no puede traspasar ningún acto normativo de la Unión. En el polo opuesto, la legitimidad de la Comisión Europea sufre un duro quebranto, al no haber garantizado debidamente un nivel de protección adecuado de los datos personales. No debemos olvidar que mantuvo en vigor la Decisión, desatendiendo la petición del Parlamento Europeo y de la autoridad alemana de protección de datos de suspender esa normativa. Por su parte, las triunfadoras indudables de este pronunciamiento son las autoridades nacionales, cuya independencia se ve consolidada en línea con la anterior jurisprudencia del Tribunal.

En suma, se trata de un pronunciamiento histórico, que marcará un antes y un después no solo en el ámbito de la protección de la privacidad, sino también en la defensa de los derechos fundamentales en el continente europeo. No todos los días se ve a un pequeño «David» (Maximilian Schrems) que, en su lucha contra Goliat (Facebook), consigue derrumbar los cimientos que habían sustentado la transferencia de datos personales entre ambas orillas del Atlántico desde el año 2000.