MARÍA ISABEL PUERTO[*] Y PIETRO SFERRAZZA TAIBI[**]

La sentencia *Schrems* del Tribunal de Justicia de la Unión Europea: un paso firme en la defensa del derecho a la privacidad en el contexto de la vigilancia masiva transnacional[***]

The *Schrems* judgment of the Court of Justice of the European Union: A firm step in the defense of the right to privacy in the context of the transnational mass surveillance

No pueden penetrar en nuestra alma. Si podemos sentir que merece la pena seguir siendo humanos, aunque esto no tenga ningún resultado positivo, los habremos derrotado.
George Orwell, *1984*

RESUMEN

Las filtraciones de Edward Snowden demostraron al mundo la existencia de programas de vigilancia masiva implementados por Estados Unidos y otros aliados. Tales programas, supuestamente, estaban dirigidos a la recopilación de información para la prevención y represión del terrorismo, pero en la práctica implicaron violaciones inaceptables al derecho fundamental a la privacidad no

[*] Candidata a doctora por el programa de Estado de Derecho y Gobernanza Global de la Universidad de Salamanca; magíster en Derecho, con mención en Derecho Internacional (Universidad de Chile, Chile); abogada; licenciada en Derecho y Ciencias Políticas y de la Administración (Universidad de Salamanca, España) y licenciada en Ciencias Jurídicas (Universidad de Chile, Chile). Profesora de Derecho Internacional Público de la Universidad Viña del Mar, Chile. Contacto: misabel.puerto82@gmail.com

[**] Doctor en Estudios Avanzados en Derechos Humanos (Universidad Carlos III de Madrid, España); abogado; licenciado en Ciencias Jurídicas (Universidad de Valparaíso, Chile). Profesor de Derecho Internacional Público de la Universidad Andrés Bello, Sede Viña del Mar, Chile. Contacto: pietrosferrazza@gmail.com

[***] Recibido el 8 de febrero de 2017, aprobado el 15 de octubre de 2017.

Para citar el artículo: Puerto, M. I. y Sferrazza Taibi, P. La sentencia *Schrems* del Tribunal de Justicia de la Unión Europea: un paso firme en la defensa del derecho a la privacidad en el contexto de la vigilancia masiva transnacional. *Derecho del Estado* n.º 40, Universidad Externado de Colombia, enero-junio de 2018, pp. 209-236. DOI: https://doi.org/10.18601/01229893.n40.09

solo de ciudadanos estadounidenses, sino de otras nacionalidades. Diversos actores de las Naciones Unidas y otras organizaciones internacionales han reaccionado mediante la elaboración de informes que manifiestan una elevada preocupación por el fenómeno de la vigilancia transnacional de masas y que pretenden ensalzar el discurso de los derechos humanos como límite contra las injerencias en la privacidad. En este contexto, el Tribunal de Justicia de la Unión Europea pronunció en el año 2015 la sentencia *Schrems* que invalidó una decisión de la Comisión Europea sobre el Acuerdo de Puerto Seguro que regulaba la transferencia de datos personales desde la Unión Europea a Estados Unidos. Este trabajo analiza críticamente dicha sentencia, porque ofrece interesantes aportaciones para la protección de los derechos a la privacidad y la protección de los datos personales, habiéndose convertido en un *leading case* de referencia obligada para la resolución de casos similares.

PALABRAS CLAVE

Vigilancia masiva, protección datos personales, derecho a la privacidad, Acuerdo de Puerto Seguro, Tribunal de Justicia de la Unión Europea.

ABSTRACT

The leaks made by Edward Snowden showed the world the existence of mass surveillance programs implemented by the United States and other allies. Such programs, supposedly, were aimed at the collection of information for the prevention and suppression of terrorism, but in practice involved unacceptable violations of the fundamental right to privacy not only of American citizens, but also of other nationalities. Various actors of the United Nations and other international organizations have responded by elaborating different reports that show concerns about the phenomenon of transnational surveillance of masses, and which seek to oppose the human rights discourse as a limit against interference to privacy. In this context, the Court of Justice of the European Union in the year 2015 delivered the Schrems sentence that reversed a decision of the European Commission on the safe harbor agreement governing the transfer of personal data from the European Union to the United States. This paper critically analyzes this sentence, because it offers interesting contributions to the protection of the rights to privacy and the protection of personal data, and has become a leading case of reference for the resolution of similar cases.

KEYWORDS

Mass surveillance, protection of personal data, right to privacy, Safe Harbor Agreement, Court of Justice of the European Union.

SUMARIO

INTRODUCCIÓN

El rápido desarrollo de las tecnologías digitales de la comunicación ha significado un cambio sin precedentes en la historia de la humanidad. Estas nuevas formas de comunicación han generado nuevos espacios de participación democrática y proporcionado a los defensores de los derechos humanos nuevas herramientas para documentar y denunciar las violaciones a los mismos. Además, la proliferación de redes sociales como Facebook o Twitter ha permitido mejorar considerablemente el acceso a la información y la comunicación en tiempo real. Sin embargo, esta era digital también presenta desafíos enormes, ya que las formas de operar de estas comunicaciones digitales han aumentado la capacidad y la posibilidad de los gobiernos, las empresas y los particulares de realizar actividades de vigilancia, interceptación y recopilación de datos de forma masiva, prácticamente sin límite alguno[1].

Concretamente las revelaciones del caso Snowden pusieron de manifiesto esos desafíos, al revelar la vulnerabilidad de las comunicaciones digitales frente a la creación de programas de vigilancia que permitieron acceder a enormes volúmenes de datos personales de particulares. Esto generó una gran preocupación a nivel internacional que se ha materializado en la adopción de diferentes iniciativas por parte de diversos actores de las Naciones Unidas y de organizaciones internacionales regionales. En efecto, la Asamblea General de las Naciones Unidas (en adelante, AG) ya ha emitido dos resoluciones sobre el tópico, exhortando a los Estados a proteger los derechos fundamentales en internet –particularmente, el derecho a la privacidad– y encargando al Alto Comisionado de las Naciones Unidas para los Derechos Humanos (en adelante, ACNUDH) la elaboración de un informe al respecto[2]. Con

1 Alto Comisionado de las Naciones Unidas para los Derechos Humanos. *El derecho a la privacidad en la era digital*. A/HRC/27/37, 30 de junio de 2014, 3.

2 AG. *El derecho a la privacidad en la era digital*, Res. 68/167, 18 de diciembre de 2013; AG. *El derecho a la privacidad en la era digital*, Res. 69/166, 18 de diciembre de 2014. Es muy probable que se adopte una tercera resolución, cuyo proyecto puede consultarse en AG, *El derecho a la privacidad en la era digital*, A/C.3/71/L.39/Rev.1, 16 de noviembre de 2016. Sobre la importancia de esta tercera resolución véase Falchetta, T. How to Bridge the Gap?

base en lo anterior, la Oficina del Alto Comisionado elaboró un interesante informe señalando que la vigilancia electrónica a gran escala configura una injerencia en el derecho a la privacidad que para ser legítima debe cumplir estándares de legalidad y proporcionalidad y debe estar sujeta a un cierto grado de supervisión en conexión con el derecho a un recurso efectivo[3]. Por su parte, el Relator Especial sobre la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión ha emitido una serie de informes sobre el impacto que las medidas destinadas a combatir el terrorismo están generando en la protección de estos derechos[4]. A nivel regional, en el ámbito europeo ya existe un caso pendiente ante el Tribunal Europeo de Derechos Humanos (en adelante, TEDH) relacionado con la participación de las agencias británicas de inteligencia en los programas de vigilancia masiva[5]. Por su parte, en el ámbito interamericano, la Relatoría Especial sobre Libertad de Expresión de la Comisión Interamericana de Derechos Humanos ha elaborado un informe sobre la libertad de expresión e internet, y ha emitido varias declaraciones, en conjunto con otras relatorías, que se refieren al impacto de los programas de vigilancia masiva sobre la protección de los derechos fundamentales[6].

Corporate and Government Surveillance Examined at the UN. *EJIL: Talk!* 7 de diciembre de 2016. [En línea]. [Consulta: 27 de enero de 2017]. Disponible en: http://www.ejiltalk.org/how-to-bridge-the-gap-corporate-and-government-surveillance-examined-at-the-un/#more-14808

3 ACNUDH, *El derecho a la privacidad en la era digital*, cit., 15 ss.

4 Véase Consejo de Derechos Humanos. *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, Frank La Rue*. A/HRC/23/40, 17 de abril de 2013; Consejo de Derechos Humanos. *Informe de Martin Scheinin, Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo*. A/HRC/14/46, 17 de mayo de 2010; Consejo de Derechos Humanos. *Informe del Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, Martin Scheinin*. A/HRC/13/37, 28 de diciembre de 2009.

5 TEDH. *Big Brother Watch v. United Kingdom*, Communicated Case, application n.º 58170/13, 2013.

6 Véase Comisión Interamericana de Derechos Humanos - Relatoría Especial para la Libertad de Expresión. *Libertad de expresión e Internet*. OEA/Ser.L/V/II, CIDH/RELE/INF. 11/13, 31 de diciembre de 2013; Relator Especial de las Naciones Unidas (ONU) para la Libertad de Opinión y de Expresión et al. *Declaración conjunta sobre libertad de expresión e internet*. En *OEA*, 1 de junio de 2011. [En línea]. [Consulta: 31 de enero de 2017]. Disponible en: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=849&lID=2; Relatoría Especial para la Libertad de Expresión et al. *Declaración conjunta sobre Wikileaks*. En *OEA*, 21 de diciembre de 2010. [En línea]. [Consulta: 31 de enero de 2017]. Disponible en: http://www.oas.org/ES/CIDH/EXPRESION/SHOWARTICLE.ASP?ARTID=889&LID=2; Relator Especial de las Naciones Unidas (ONU) para la Libertad de Opinión y de Expresión et al. *Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión*. En *OEA*, 2 de junio de 2013. [En línea]. [Consulta: 31 de enero de 2017]. Disponible en: http://www.oas.org/ES/CIDH/EXPRESION/SHOWARTICLE.ASP?ARTID=926&LID=2; Relator Especial de las Naciones Unidas (ONU) para la Libertad de Opinión y de Expresión et al. *Declaración conjunta sobre la libertad de expresión y las respuestas a las situaciones de conflicto*. En *OEA*, 4 de mayo de 2015. [En línea]. [Consulta: 31 de enero de 2017]. Disponible en: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=987&lID=2

En este contexto, de lograr un equilibrio entre las políticas de seguridad nacional y el respeto a la vida privada, la sentencia *Schrems* se configura como un caso histórico que culmina con la declaración de invalidez del Acuerdo de Puerto Seguro por no respetar derechos fundamentales consagrados en el marco normativo comunitario. Sobre esa base, el objetivo de este trabajo es analizar la sentencia emitida por el Tribunal de Justicia de la Unión Europea (en adelante, TJUE) denominada *Maximilian Schrems y Data Protection Commissioner*, del 6 de octubre de 2015[7]. Para ello, en primer lugar se llevará a cabo un análisis del contexto normativo en el que se pronunció la sentencia con el objetivo de tener una mejor comprensión de la misma. En segundo lugar, se señalarán brevemente los hechos, para pasar a continuación a analizar los argumentos de fondo de la sentencia, donde se abordarán dos aspectos fundamentales: por un lado, las facultades que tienen las autoridades nacionales de control de protección de datos frente a una decisión de la Comisión Europea, y por otro, los principales fundamentos que esgrime el TJUE para declarar la invalidez de la decisión de la Comisión a la luz de la Carta de Derechos Fundamentales de la Unión Europea (en adelante, CDFUE)[8].

1. CONTEXTUALIZACIÓN NORMATIVA

En tanto que el caso *Schrems* versa sobre la legalidad de las transferencias de datos a Estados Unidos bajo el sistema establecido por el Acuerdo de Puerto Seguro (*Safe Harbor Agreement*), es necesario aludir al contexto normativo europeo sobre protección de datos para comprender adecuadamente la sentencia. En este sentido, se torna imprescindible mencionar tres artículos consagrados en la CDFUE. Por un lado, el artículo 7 que protege el derecho a la privacidad[9]. La misma CDFUE regula de manera explícita en su artículo 8 el derecho a la protección de los datos de carácter personal[10]. Finalmente, cabe

7 TJUE. *Maximilian Schrems y Data Protection Commissioner*, C-362/14, 6 de octubre de 2015.

8 UE. *Carta de los Derechos Fundamentales de la Unión Europea*. (2016/C 202/02), versión consolidada, *Diario Oficial de la Unión Europea*, C202/1, 17 de junio de 2016. Si bien esta Carta fue formalmente proclamada en Niza en diciembre de 2000 por el Parlamento Europeo, el Consejo y la Comisión, fue a partir de diciembre de 2009, con la entrada en vigor del Tratado de Lisboa, que se convirtió en un documento constitucional que obliga jurídicamente a las instituciones de la UE y los Estados miembros. Véase FABBRINI, F. Human Rights in the Digital Age: The European Court of Human Rights in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States. *Human Rights in the Digital Age*, 2015(28), 70.

9 Art. 7 CDFUE: "Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones".

10 Art. 8.1 y 8.2 CDFUE: "1. Toda persona tiene derecho a la protección de los datos de carácter personal que la 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 la conciernan y a su rectificación". Es

señalar que la Carta también regula el derecho de tutela judicial efectiva en su artículo 47[11].

Confirmando precisamente la centralidad que la protección de datos juega en el orden jurídico de la Unión Europea (en adelante, UE), el artículo 16 del Tratado de Funcionamiento de la Unión Europea (en adelante, TFUE) determina que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan, y encomienda al Parlamento Europeo y al Consejo que establezcan las normas sobre protección de las personas físicas respecto del tratamiento de datos de carácter personal y las normas relativas a la libre circulación de dichos datos[12]. En relación con lo anterior, cabe señalar que recientemente ha entrado en vigor el nuevo Reglamento general de protección de datos que sustituyó a la anterior Directiva 95/46/CE sobre la materia[13]. La entrada en vigor de este Reglamento, sin duda, ha supuesto un paso decisivo en la protección de datos personales en el ámbito comunitario al acabar con la fragmentación normativa existente entre los Estados miembros fruto de la aplicación de la Directiva y estableciendo un marco regulatorio más transparente y uniforme que imponga a los responsables del tratamiento de datos personales el mismo nivel de obligaciones[14].

posible apreciar que esta disposición establece una orientación básica sobre el procesamiento de datos, incluida la necesidad de la limitación de la finalidad, el control independiente por una autoridad supervisora y la disponibilidad de un fundamento jurídico establecido por la ley, así como los derechos de acceso y rectificación de sus datos personales.

11 Art. 47 CDFUE: "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.

"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".

12 UE. *Tratado de Funcionamiento de la Unión Europea*. (2016/C 202/01), versión consolidada, *Diario Oficial de la Unión Europea*, C202/2, 17 de junio de 2016, art. 16: "1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan.

"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 libre circulación de estos datos. El respeto de dichas normas estará sometido al control de autoridades independientes".

13 UE. *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos que viene a derogar y sustituir a la Directiva 95/46/CE*, *Diario Oficial de la Unión Europea*, L119, 4 de mayo de 2016. Si bien el Reglamento entró en vigor a los veinte días desde su publicación –conforme a lo establecido en su artículo 99–, solo será aplicable a partir del 25 de mayo de 2018, con el fin de que los Estados puedan realizar todas las modificaciones que sean necesarias para cumplir con sus disposiciones.

14 Díaz Díaz, E. El nuevo Reglamento General de Protección de Datos de la Unión Europea

Sin perjuicio de lo anterior, debe aclararse que la sentencia *Schrems* razona sobre la base de la normativa fundamental vigente al momento de los hechos, esto 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 (en adelante, Directiva)[15]. Esta Directiva establecía un régimen normativo exhaustivo en relación con el tratamiento de los datos personales concernientes a personas naturales en el contexto de las transacciones comerciales aprobadas bajo el marco del mercado común europeo. Entre otras cosas, permitía la transferencia de datos personales a países no comunitarios en la medida en que estos ofrecieran un nivel adecuado de protección de la vida privada[16]. Conforme a su artículo 25.6, la Comisión era la encargada de hacer constar cuando un país cumplía con un nivel adecuado de protección, teniendo en consideración tanto su legislación interna como los compromisos internacionales que hubiera asumido[17].

Bajo este marco normativo, la Comisión celebró un acuerdo con el Departamento de Comercio de Estados Unidos que culminó con la adopción de la Decisión 2000/520 (en adelante, Decisión), que vinculaba a todos los Estados miembros y que fue medular para la resolución del caso *Schrems*[18]. Mediante esta Decisión se estableció un sistema de autocertificación, por el cual las empresas estadounidenses se comprometían a gestionar los datos personales que fueran transferidos a Estados Unidos bajo el amparo de los

y sus consecuencias jurídicas para las instituciones. *Revista Aranzadi Doctrinal*, 2016(6), 155-190.

15 UE. *Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*, *Diario Oficial de las Comunidades Europeas*, L281, 23 de noviembre de 1995. Sobre esta Directiva, véase Piroddi, P. I trasferimenti di dati personali verso paesi terzi dopo la sentenza Schrems e nel nuovo regolamento generale sulla protezione dati. *Diritto dell'informazione e dell'informatica*, 2015, 31(4-5), 830 ss.

16 Directiva, cit., consid. 56: "Considerando que los flujos transfronterizos de datos personales son necesarios para el desarrollo del comercio internacional; que la protección de las personas garantizada en la Comunidad por la presente Directiva no se opone a la transferencia de datos personales a terceros países que garanticen un nivel de protección adecuado".

17 Directiva, cit., art. 25.6: "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".

18 Comisión Europea. *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*, *Diario Oficial de las Comunidades Europeas*, n.º 125, 25 de agosto de 2000.

principios de puerto seguro[19]. Una vez que las empresas autocertificaban su adhesión a estos principios se presumía que cumplían con el nivel de protección adecuado exigido por la Directiva[20].

Sin embargo, a raíz de las revelaciones de Snowden, la Comisión advirtió en dos comunicaciones de 2013, dirigidas al Parlamento Europeo y al Consejo, que muchas empresas autocertificadas no cumplían con los principios de puerto seguro, señalando que este incumplimiento permitió a las autoridades estadounidenses acceder a los datos personales transferidos a su territorio y tratarlos de manera incompatible con las finalidades de esa transferencia, yendo más allá de lo que era estrictamente necesario y proporcionado para la protección de la seguridad nacional[21]. Del mismo modo, la Comisión apreció en dichas comunicaciones que las personas afectadas ni siquiera 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 supre-

19 El *Safe Harbor Agreement* está formado por un conjunto de siete principios que garantizan un nivel adecuado de protección de los datos personales transferidos desde la UE a empresas establecidas en Estados Unidos. Dichos principios son: 1) Notificación, que obliga a las empresas adheridas a los principios de puerto seguro a informar a los interesados de la finalidad para la cual han sido recopilados sus datos así como de la identificación del responsable del fichero, con el objeto de que estos puedan ejercer sus derechos de acceso, rectificación o supresión; 2) Opción, que permite al titular decidir sobre la finalidad y el destino de sus datos de carácter personal; 3) Transferencia ulterior, conforme al cual solo se permite la transferencia de datos cuando las entidades o países destinatarios ofrezcan como mínimo el mismo nivel de protección de la vida privada que el requerido en el Acuerdo de Puerto Seguro; 4) Seguridad, en cuanto las empresas adheridas deben adoptar todas las precauciones razonables para evitar que se haga un mal uso, divulgue, modifique, pierda, destruya o realice una consulta no autorizada sobre la información recopilada. 5) Integridad de los datos, en cuya virtud la información personal recopilada no puede ser utilizada de manera incompatible con los fines que motivaron su recogida y se deberán adoptar todas las medidas razonables para que los datos tengan fiabilidad para el uso previsto y sean exactos, completos y actuales; 6) Acceso, conforme al cual los particulares deben tener acceso a la información recopilada y deben existir mecanismos que permitan a los mismos solicitar la rectificación o supresión cuando la información recopilada sea inexacta; 7) Aplicación, referido a la necesidad de articular mecanismos y recursos independientes a los que los particulares puedan acudir en caso de incumplimiento de estos principios y que se establezcan sanciones contra la entidad incumplidora. Véase Álvarez Caro, M. y Recio Gayo, M. Hacia un acuerdo Safe Harbor renovado para la transferencia internacional de datos entre EE.UU y la UE. *Papeles de Derecho Europeo e Integración Regional*. Madrid, IDEIR, 2015, n.º 25. [En línea]. [Consulta: 25 de enero 2017]. Disponible en: https://www.ucm.es/data/cont/docs/595-2015-06-15-Binder218.pdf, 86.

20 Uría Gavilán, E. 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*. *Revista de Derecho Comunitario Europeo*, enero/abril 2016(53), 265.

21 Véase Comisión Europea. *Comunicación al Parlamento Europeo y al Consejo*. *Restablecer la confianza en los flujos de datos entre la UE y EE.UU*. COM(2013) 846 final, 27 de noviembre de 2013, 4-5; Comisión Europea. *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, 27 de noviembre de 2013, 17-18.

sión[22]. Tales comunicaciones son relevantes dado que el TJUE las incluyó en el marco jurídico que sirvió de base para la resolución de las cuestiones de fondo del caso *Schrems*[23].

2. LOS HECHOS DEL CASO: ¿UNA MUERTE ANUNCIADA DE LOS PRINCIPIOS DE PUERTO SEGURO?

Los hechos del caso dicen relación con una reclamación presentada ante la autoridad irlandesa de protección de datos personales –el Comisario Irlandés de Protección de Datos (*Data Protection Commissioner*)– por parte de Maximilian Schrems, un joven jurista austriaco residente en Irlanda. Tal como se menciona brevemente en la sentencia, el caso tiene directa relación con las filtraciones de Edward Snowden a propósito de algunos programas de vigilancia masiva implementados por la Agencia Nacional de Seguridad de Estados Unidos (National Security Agency o NSA) y otras agencias colaboradoras, como el Cuartel General de Comunicaciones del Gobierno del Reino Unido (Government Communications Headquarters o GCHQ)[24]. Con posterioridad a los atentados del 11 de septiembre y con la supuesta finalidad de prevenir ataques terroristas, la implementación de estos programas permitió recolectar de manera masiva los datos personales de millones de usuarios de los servicios de telecomunicación a lo largo y ancho del globo[25].

La tecnología utilizada para tal efecto razonaba sobre la lógica del *Big Data*, con lo cual los datos no eran recopilados selectivamente, sino a gran escala, incluyendo la información de personas no sospechosas de cometer o planificar un delito. Los datos recopilados eran procesados con el supuesto objetivo de recabar información útil para la prevención y sanción de delitos terroristas[26]. El alcance de estas operaciones era transfronterizo, afectando

22 Comunicación COM(2013) 847, cit., 18-19.

23 TJUE, *Schrems*, cit., 11 ss.

24 Para el debate sobre las ventajas y desventajas de las filtraciones de información, desde el punto de vista de la democracia y del Estado de derecho, véase COLE, D. The Three Leakers and what to do about them. *The New York Review of Books* [En línea], 6 de febrero de 2014. Vol. 61(2). [En línea]. [Consulta: 16 de enero de 2017]. Disponible en: http://www.nybooks.com/articles/2014/02/06/three-leakers-and-what-do-about-them/

25 La vigilancia transnacional (*foreign surveillance*) es una expresión que debe ser entendida en sentido amplio que permita comprender la recopilación de información de inteligencia mediante la realización de un diverso espectro de actividades, tales como la observación audiovisual, la interceptación de cualquier tipo de comunicación y la recopilación y procesamiento de datos. Al respecto, véase MILANOVIC, M. Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age. *Harvard International Law Journal*, winter 2015, 56(1), 86. Para el detalle de los programas de espionaje implementados por estas agencias, véase BOWDEN, C. *The US Surveillance Programmes and their Impact on EU Citizens' Fundamental Rights*. Brussels: European Parliament - Directorate-General for Internal Policies, 2013, 12-15.

26 Sobre las técnicas contemporáneas de espionaje que permiten acceder masivamente a los datos personales, véase la didáctica explicación de COMELLA, C. Alcune considerazioni sugli

no solo a ciudadanos norteamericanos, sino también a todo el mundo. Para coronar lo anterior, los programas eran puestos en marcha con absoluto secreto y casi sin garantías de revisión judicial, contando además con un sustento jurídico formal en la normativa interna[27].

Pues bien, el joven Schrems era usuario de Facebook, una de las empresas de telecomunicación más importantes del mundo[28]. Facebook tiene una importante filial en Irlanda, Facebook Ireland, que se encarga de transferir a Estados Unidos los datos personales de todos los usuarios europeos[29].

En su reclamación ante el Comisario Irlandés de Protección de Datos, Schrems alegaba que las revelaciones de Snowden demostraban que Estados Unidos no aseguraba un nivel adecuado de protección respecto de los datos personales que se transferían a ese país. Con base en lo anterior, Schrems solicitó que se prohibiera la transferencia de datos a Estados Unidos[30]. El Comisario Irlandés rechazó la solicitud, argumentando que la Decisión de la Comisión presumía que Estados Unidos cumplía con un nivel de protección adecuado. Además, indicó que no tenía el deber de investigar los hechos, dado que el demandante no había aportado pruebas suficientes para demostrar que la NSA había accedido efectivamente a sus datos personales[31].

Tras esta primera derrota, Schrems presentó un recurso ante la Alta Corte de Irlanda. A diferencia del pronunciamiento anterior, este tribunal consideró que las revelaciones de Snowden habían demostrado injerencias excesivas de Estados Unidos en el tratamiento de los datos personales. Además, estimó que la interpretación de la Decisión de la Comisión Europea a la luz de la Directiva 95/46/CE planteaba un problema de implementación del derecho de la Unión

aspetti tecnologici della sorveglianza di massa. A margine della sentenza 'Safe Harbor' della Corte di Giustizia dell'Unione Europea. *Diritto dell'informazione e dell'informatica*, 2015. Vol. 31(4-5), 724 ss.

27 Para una reseña de la normativa interna que sirvió de base a los programas de vigilancia estadounidense, véase MARGULIES, P. The NSA in Global Perspective: Surveillance, Human Rights and International Counterterrorism. *Fordham Law Review*, 2014, 82(5), 2140-2142; RESTA, G. La sorveglianza elettronica di massa e il conflitto regolatorio USA/UE. *Diritto dell'informazione e dell'informatica*, 2015, 31(4-5), 700-704, enfocándose en las interpretaciones jurisprudenciales de la Cuarta Enmienda de la Constitución norteamericana.

28 TJUE, *Schrems*, cit., 26.

29 TJUE, *Schrems*, cit., 27. Véase DARCY, S. Battling for the Rights to Privacy and Data Protection in the Irish Courts. *Utrecht Journal of International and European Law*, 2015. Vol. 31(80), 131, explicando que Facebook ha establecido su filial en Irlanda, al igual que otras empresas multinacionales, porque las tasas tributarias y la regulación sobre datos personales son menos exigentes que en el resto de Europa.

30 TJUE, *Schrems*, cit., 28. Resulta interesante revisar la web de la organización creada por Schrems denominada "Europe versus Facebook", ya que da cuenta de todas las acciones judiciales realizadas por este activista. Disponible en: http://europe-v-facebook.org/EN/Objectives/objectives.html [Consulta: 14 de septiembre de 2016].

31 Véase TJUE, *Schrems*, cit., 29; Alta Corte de Irlanda (High Court). *Schrems v. Data Protection Commissioner* [2014] IEHC 213, 30-31.

Europea por parte de los Estados miembros con base en el artículo 51 CDFUE[32], con lo cual decidió elevar una cuestión prejudicial al TJUE[33]. Mediante dicho mecanismo la Alta Corte planteó lo siguiente:

1) En primer lugar, consultó si el Comisario Irlandés estaba vinculado por la protección de los derechos fundamentales consagrados en la Carta de Niza, a pesar de que la Decisión presumía que Estados Unidos garantizaba un nivel adecuado de protección.

2) En segundo lugar, planteó si el Comisario Irlandés podía iniciar una investigación independiente, sin perjuicio de lo dispuesto en esta Decisión[34].

El 23 de septiembre de 2015, el Abogado General Yves Bot emitió sus conclusiones[35] y el 6 de octubre del mismo año, actuando como Gran Sala, el TJUE dictó la sentencia objeto de análisis.

Habiéndose explicado la normativa relevante para el caso y los hechos que lo promovieron, se analizan a continuación las cuestiones de fondo que sirvieron de base para la invalidación de la Decisión, y que son atinentes al debate sobre la defensa de los derechos fundamentales en el contexto de la vigilancia transnacional.

32 CDFUE, cit., art. 51.1: "Las disposiciones de la presente Carta están dirigidas a las instituciones y órganos de la Unión, respetando el 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".

33 Alta Corte de Irlanda (High Court). *Schrems v. Data Protection Commissioner*, cit., 60. La cuestión prejudicial está regulada en el artículo 267 TFUE, cit., en los siguientes términos: "El Tribunal de Justicia de la Unión Europea será competente para pronunciarse, con carácter prejudicial: a) sobre la interpretación de los Tratados;

"b) sobre la validez e interpretación de los actos adoptados por las instituciones, órganos u organismos de la Unión;

"Cuando se plantee una cuestión de esta naturaleza ante un órgano jurisdiccional de uno de los Estados miembros, dicho órgano podrá pedir al Tribunal que se pronuncie sobre la misma, si estima necesaria una decisión al respecto para poder emitir su fallo.

"Cuando se plantee una cuestión de este tipo en un asunto pendiente ante un órgano jurisdiccional nacional, cuyas decisiones no sean susceptibles de ulterior recurso judicial de Derecho interno, dicho órgano estará obligado a someter la cuestión al Tribunal.

"Cuando se plantee una cuestión de este tipo en un asunto pendiente ante un órgano jurisdiccional nacional en relación con una persona privada de libertad, el Tribunal de Justicia de la Unión Europea se pronunciará con la mayor brevedad".

34 Véase TJUE, *Schrems*, cit., 36; Alta Corte de Irlanda (High Court). *Schrems v. Data Protection Commissioner*, cit., 71.

35 TJUE. *Conclusiones del Abogado General*, Sr. Yves Bot, Asunto C-362/14, 23 de septiembre de 2015.

3. LAS AUTORIDADES NACIONALES DE CONTROL DE DATOS PERSONALES COMO GUARDIANES DE LOS DERECHOS FUNDAMENTALES

Las autoridades nacionales de control han sido creadas en virtud del artículo 28 de la Directiva[36] y constituyen un elemento esencial para la protección de las personas frente al tratamiento de sus datos personales[37]. Precisamente, estas autoridades son las encargadas de realizar un control eficaz y fiable del cumplimiento de las normas de la UE sobre protección de datos personales. Para que estas autoridades puedan desempeñar su función de manera eficaz es indispensable que se trate de órganos independientes. A este respecto, el TJUE ha sido constante en su jurisprudencia en determinar que "esta independencia excluye no sólo cualquier influencia que pudieran ejercer los organismos sujetos a control, sino también todo orden o influencia externa, directa o indirecta, que pudiera poner en peligro el cumplimiento de la tarea que corresponde a dichas autoridades de establecer un justo equilibrio entre la protección del derecho a la intimidad y la libre circulación de datos personales"[38]. En este sentido, el TJUE ha dictado varios fallos en que se determina la violación por parte de algunos Estados miembros de la Directiva por no garantizar la "total independencia" de estas autoridades en el ejercicio de sus funciones[39].

Cabe señalar también que dichas autoridades disponen de una amplia gama de facultades, en particular: facultades de investigación, como la de recabar toda la información necesaria para el cumplimiento de su misión de control; facultades efectivas de intervención, como la de prohibir provisional o definitivamente un tratamiento de datos; e incluso, tienen la capacidad de comparecer en juicio[40]. En este punto es interesante destacar que el Tribunal

36 Directiva, cit., art. 28. 1: "Los Estados miembros dispondrán que una o más autoridades públicas se encarguen de vigilar la aplicación en su territorio de las disposiciones adoptadas por ellos en aplicación de la presente Directiva".

37 Véase TJUE, *Comisión Europea v. República Federal de Alemania*, C-518/07, 9 de marzo de 2010, 23; TJUE, *Comisión Europea v. República de Austria*, C-614/10, 16 de octubre de 2012, 37; TJUE, *Comisión Europea v. Hungría*, C-288/12, 8 de abril 2014, 48.

38 Véase TJUE, *Comisión Europea v. República Federal de Alemania*, cit., 19, 25, 30 y 50; *Comisión Europea v. República de Austria*, cit., 41 y 43; *Comisión Europea v. Hungría*, cit., 51.

39 URIA GAVILÁN, ob. cit., 272. Este sería el caso, por ejemplo, de Alemania, en donde el Tribunal determinó que el excesivo control que podían ejercer los *Länder* respecto a las autoridades de control, incluso anulando sus decisiones, no era compatible con las exigencias de total independencia establecidas en la Directiva comunitaria (TJUE, *Comisión Europea v. República Federal de Alemania*, cit., 31-36). En esta misma línea, el Tribunal ha señalado que la normativa austriaca, al establecer como autoridad de control a un funcionario federal sujeto a la autoridad de la Cancillería Federal y, por lo tanto, sometido a su supervisión jerárquica, impedía al mismo ejercer sus funciones con total independencia, tal como lo exige la norma comunitaria (TJUE, *Comisión Europea v. República de Austria*, cit., 48-66). Finalmente, Hungría fue condenada por poner fin antes de tiempo al mandato de su autoridad de control sin que existiese una razón objetiva que justificara su destitución (TJUE, *Comisión Europea v. Hungría*, cit., 47-64).

40 Estas facultades están enumeradas de forma no exhaustiva por el artículo 28.3 de la Directiva 95/46/CE.

ha determinado en el caso *Weltimmo* que las autoridades de control pueden ejercer dichas facultades no solo sobre empresas domiciliadas en su territorio, sino también sobre aquellas empresas que al realizar tratamientos de datos personales ejerzan, mediante una instalación estable, una actividad efectiva y real en el territorio del Estado de esa autoridad de control[41]. Por ende, dicha sentencia maneja una concepción bastante flexible de "establecimiento"[42]. Con esta decisión el Tribunal utilizó el principio de territorialidad para abordar eficazmente el problema de que algunas empresas creen una realidad empresarial alternativa para vincularse a la ley y al régimen de ejecución de otro Estado miembro más indulgente, puesto que en la actualidad no todas las autoridades nacionales de protección de datos son igualmente activas y, además, existe una cierta disparidad en la transposición de la Directiva entre los distintos Estados miembros[43].

Precisamente en relación con las facultades de estas autoridades, la cuestión principal que trata de dilucidar el Tribunal en el caso *Schrems* es si debe interpretarse que la Decisión de la Comisión impide que una autoridad de control nacional, como el Comisario Irlandés de Protección de Datos, examine la solicitud de una persona con el fin de comprobar si una transferencia de datos personales desde el Estado miembro hacia un tercer Estado respeta las exigencias establecidas por la Directiva. A este respecto, el Tribunal declaró que aun cuando la Comisión ha adoptado una Decisión donde se presume la existencia de un nivel adecuado de protección, las autoridades nacionales de control estarían investidas de competencia para examinar una reclamación con el objeto de verificar si la transferencia de datos de una persona a un tercer Estado cumple con los requisitos establecidos por la Directiva. Lo anterior

41 TJUE, *Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*, C-230/14, 1 de octubre de 2015, 41, 49, 57 y 59.

42 TJUE, *Weltimmo*, cit., 33: "Además, de las puntualizaciones aportadas por la autoridad húngara de control se desprende que Weltimmo dispone de un representante en Hungría, que se menciona en el registro de sociedades eslovaco con una dirección en Hungría y que intentó negociar con los anunciantes el pago de los créditos impagos. Dicho representante sirvió de enlace entre la citada sociedad y los denunciantes y la representó en los procedimientos administrativo y judicial. Por añadidura, la referida sociedad abrió una cuenta bancaria en Hungría, destinada al cobro de sus créditos, y utiliza un apartado de correos en el territorio de dicho Estado miembro para la gestión de sus asuntos corrientes. Estos factores, que corresponde al órgano jurisdiccional remitente comprobar, pueden demostrar, en una situación como la controvertida en el litigio principal, la existencia de un 'establecimiento', a efectos del artículo 4, apartado 1, letra a), de la Directiva 95/46". Al respecto véase Woods, L. Data Protection: The CJEU Clarifies the Applicable Law and Jurisdiction. *EU Law Analysis*, 13 de octubre de 2015. [En línea]. [Consulta: 24 de enero de 2017]. Disponible en: http://eulawanalysis.blogspot.cl/2015/10/data-protection-cjeu-clarifies.html.

43 Gryffroy, P. Taking a Look at Two Cases in the Margin of the CJEU's 'Privacy Spring', before and after the General data Protection Regulation: Weltimmo and Bara. *Jean-Monnet-Saar/Europarecht online*, 21 de junio de 2016. [En línea]. [Consulta: 16 de enero de 2017]. Disponible en: http://jean-monnet-saar.eu/?p=1453

tiene explicación en el hecho de que las autoridades de control siguen siendo las máximas responsables de supervisar el procesamiento de datos sobre su territorio, lo que incluye el control sobre la transferencia de datos personales fuera de la UE[44]. Además, el tribunal señaló que la Directiva, que debe interpretarse a la luz de la Carta, no contiene ninguna disposición que impida la supervisión por parte de dichas autoridades respecto de la transferencia de datos a terceros países sujetos a una decisión que establece un nivel de protección adecuado[45].

A su vez, sin embargo, el TJUE afirmó que es el único órgano competente para declarar la invalidez de un acto normativo comunitario, y mientras la Decisión no haya sido declarada invalida por él, las autoridades de control no pueden adoptar medidas contrarias a la misma por tratarse de una norma obligatoria para todos los Estados miembros destinatarios y vinculante para sus órganos[46]. Pese a la falta de competencia para invalidar un acto comunitario, es relevante destacar que las autoridades de control, frente a una solicitud que impugna la compatibilidad de la Decisión con el derecho a la vida privada, deben examinar la referida solicitud con toda la "diligencia exigible"[47]. El TJUE entiende que la expresión "diligencia exigible" conlleva dos situaciones. La primera se refiere al hecho de que la autoridad llegue a la conclusión de que los datos alegados en apoyo de esa solicitud son infundados y la desestime por ello. En este caso, la persona que haya presentado la solicitud debe disponer de recursos jurisdiccionales que le permitan impugnar la decisión ante los tribunales nacionales. Esos tribunales están obligados a suspender el procedimiento y plantear al TJUE una cuestión prejudicial de validez si estiman que uno o varios de los motivos de invalidez alegados por las partes o conocidos de oficio son fundados[48]. Por el contrario, si dicha autoridad considera fundadas las alegaciones debe tener la capacidad para comparecer ante los tribunales nacionales para que estos, si concuerdan, planteen al TJUE una cuestión prejudicial sobre la validez de la Decisión de la Comisión[49]. Como ya se ha mencionado en algún comentario sobre la sentencia, no parece muy afortunado que el TJUE no tome en cuenta la posibilidad de que las autoridades nacionales de control pudieran pedir a la Comisión que modifique su Decisión si consideran sospechosa la validez de la misma, sin la necesidad de comparecer ante un tribunal nacional[50].

44 TJUE, *Schrems*, cit., 44-47
45 Ibid., 51-55.
46 Ibid., 51-52.
47 Ibid., 61-63.
48 Ibid., 64.
49 Ibid., 65.
50 PEERS, S. The Party's Over: EU Data Protection Law after the Schrems Safe Harbor Judgment. *EU Law Analysis*, 7 de octubre de 2015. [En línea]. [Consulta: 16 de enero de 2017]. Disponible en: http://eulawanalysis.blogspot.cl/2015/10/the-partys-over-eu-data-protection-law.html.

Finalmente, es interesante señalar que si bien el TJUE, en aras de la seguridad jurídica, se reserva la facultad exclusiva de declarar la invalidez de cualquier norma comunitaria, en esta sentencia viene a reforzar y consolidar el papel de las autoridades nacionales de control como guardianes de los derechos fundamentales en lo que respecta a la protección de datos personales, otorgándoles competencias claras frente a una decisión de la Comisión Europea que pueda vulnerar dichos derechos. Dichas competencias son las siguientes: 1) examinar las denuncias de particulares relativas al tratamiento de sus datos personales por parte de otros países; 2) llevar los casos ante los tribunales nacionales para cuestionar la validez de la adecuación de las decisiones; y, 3) suspender la transferencia de datos personales a otros países cuando crean que no cumplen con un nivel adecuado de protección[51].

4. EL PAPEL DE LOS DERECHOS FUNDAMENTALES EN LA INVALIDACIÓN DE UNA NORMA COMUNITARIA

Sin duda, el aspecto más llamativo de la sentencia *Schrems* radica en que la invalidación de una norma de derecho comunitario –como la Decisión de la Comisión Europea– se haya fundamentado en una argumentación coherente con el discurso de los derechos fundamentales, y en que para tal efecto se haya tomado como base normativa la CDFUE. Los derechos fundamentales que se consideraron vulnerados en el caso son el derecho a la privacidad y el derecho a la tutela judicial efectiva. Resulta algo extraño que la sentencia *Schrems* no haya considerado vulnerado el derecho a la protección de datos de carácter personal, si bien en su argumentación alude reiteradamente a la noción de "dato personal" –sin definirla[52].

La relación y distinción entre el derecho a la privacidad y el derecho a la protección de datos personales no ha sido abordada adecuadamente en la jurisprudencia del TJUE y del TEDH. Ambos derechos parecen tener ámbitos de aplicación que en parte se solapan y en parte difieren, ya que la privacidad incluye *algunos* datos de una persona, pero no engloba necesariamente *todos* los datos personales[53]. Finocchiaro argumenta que el contenido del derecho a la protección de datos personales es muy amplio, en cuanto permite a su

51 Škrinjar, M. Schrems v. Data Protecion Commissioner (Case C-362/14): Empowering National Data Protection Authorities. *Croatian Yearbook of European Law and Policy*, 2015(11), 265.

52 Tracol, X. 'Invalidator' Strikes Back: the Harbor has Never Been Safe. *Computer Law & Security Review*, 2016, 32(2), 355. Véase TJUE, *Conclusiones del Abogado General, Sr. Yves Bot*, cit., 215 y 236, defendiendo una posición distinta, al afirmar que el derecho a la protección de los datos personales había sido vulnerado desde la óptica del principio de proporcionalidad.

53 Para profundizar en las diferencias entre ambos derechos a la luz la jurisprudencia del TEDH y la TJUE, véase Kokott, J. y Sobotta, C. The Distinction between Privacy and Data Protection in the Jurisprudence of the CJEU and the EctHR. *International Data Privacy Law*, 2013, 3(4), 222-228.

titular controlar el conjunto de las informaciones que se refieren a él, que configuran su reflejo y delimitan su ser en la sociedad de la información. De ese modo, el derecho a la protección de los datos personales no es una libertad negativa como el derecho a la privacidad, sino un derecho a la autodeterminación informativa, o sea, una libertad positiva que permite ejercer un control con respecto al flujo de las informaciones sobre la propia persona[54]. Con independencia de estas reflexiones, consideramos que en su jurisprudencia futura el TJUE debe intentar trazar una distinción conceptual entre ambos derechos. Dicho esto, a continuación se comenta de qué manera *Schrems* consideró infringido el contenido esencial del derecho a la privacidad y del derecho a la tutela judicial efectiva.

4.1. La vulneración del contenido esencial del derecho a la privacidad

La Decisión de la Comisión Europea presumía que Estados Unidos cumplía con el estándar de nivel de protección adecuado exigido por la Directiva. Cabe preguntarse qué se entiende por "adecuado", dado que la Directiva no otorgaba una definición[55]. Interpretando la Directiva, la sentencia *Schrems* consideró que la valoración del estándar de protección adecuado debía realizarse a la luz de varias circunstancias relacionadas con la transferencia de datos, todas ellas indicadas en el artículo 25.2[56]. En opinión del TJUE, el criterio más relevante para determinar si se cumplía con la protección adecuada era la protección a los derechos fundamentales ofrecida por el tercer país, sobre todo, la protección del derecho a la vida privada[57].

Para satisfacer este estándar, el Tribunal estimó que el tercer país no debía ofrecer un nivel de protección idéntico al existente en la UE, sino que

54 FINOCCHIARO, G. La giurisprudenza della Corte di Giustizia in materia di dati personali da *Google Spain* a *Schrems*. *Diritto dell'informazione e dell'informatica*, 2015, 31(4-5), 783-784.

55 POLLICINO, O. y BASSINI, M. La Carta dei Diritti Fondamentali dell'Unione Europea nel *reasoning* dei giudici di Lussemburgo. *Diritto dell'informazione e dell'informatica*, 2015, 31(4-5), 751.

56 TJUE, *Schrems*, cit., 70. Véase Directiva 95/46/CE, cit., art. 25.2: "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".

57 TJUE, *Schrems*, cit., 71-72. Véase Directiva 95/46/CE, cit., art. 25.6: "6. La Comisión podrá hacer constar, de conformidad con el procedimiento previsto en el apartado 2 del artículo 31, que un país tercero garantiza un nivel de protección adecuado de conformidad con el apartado 2 del presente artículo, a la vista de su legislación interna o de sus compromisos internacionales, suscritos especialmente al término de las negociaciones mencionadas en el apartado 5, a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas".

debía ser "sustancialmente equivalente". Para calificar esta cuestión era indispensable tener en consideración lo prescrito en la CDFUE, porque de lo contrario los ciudadanos de la UE estarían expuestos a una vulneración de sus derechos fundamentales mediante la transferencia de datos a un tercer país[58]. Con base en lo anterior se entendió que el ordenamiento jurídico del tercer país podía ofrecer medios distintos de protección, pero en la práctica su nivel de eficacia debía ser sustancialmente equivalente al nivel de protección asegurado en la UE[59].

Pues bien, para determinar si hubo una infracción al derecho a la privacidad consagrado en el artículo 7 CDFUE, la sentencia *Schrems* razonó sobre la base de un doble eje argumentativo. En primer término, aclaró que se había producido una injerencia en el ejercicio de este derecho en perjuicio de los ciudadanos europeos. En segundo lugar, declaró que dicha injerencia significó una vulneración del contenido esencial del derecho a la privacidad. Ambos argumentos se analizan en profundidad a continuación.

Para determinar si hubo una injerencia, la sentencia *Schrems* realizó una valoración del ordenamiento jurídico interno de Estados Unidos a fin de determinar si protegía adecuadamente los datos personales transferidos desde Europa[60]. En principio, el Tribunal descartó que el sistema de autocertificación norteamericano fuese *per se* contrario al estándar de protección adecuado[61]. Sin embargo, la Decisión consagraba la primacía de las exigencias de seguridad nacional y de la legislación interna estadounidense por sobre los principios de puerto seguro[62]. Eso significaba que las empresas autocertificadas debían dejar de cumplir estos principios si eran contradictorios con la normativa interna estadounidense[63]. En opinión del Tribunal, esta situación daba lugar

58 TJUE, *Schrems*, cit., 73. Sobre el papel de la CDFUE en la interpretación del nivel de protección adecuado, véase POLLICINO Y BASSINI, ob. cit., 746, 752 y 753; ECKES, C. y ABAZI, V. Safe Harbor Case: Safeguarding European Fundamental Rights or Creating a Patchwork of National Data Protection? *UK Constitutional Law Blog,* 9 de octubre de 2015. [En línea]. [Consulta: 29 de septiembre de 2016]. Disponible en: https://ukconstitutionallaw.org/2015/10/09/christina-eckes-and-vigjilenca-abazi-safe-harbour-case-safeguarding-european-fundamental-rights-or-creating-a-patchwork-of-national-data-protection/.

59 TJUE, *Schrems*, cit., 74. Véase TJUE, *Conclusiones del Abogado General*, Sr. Yves BOT, cit., 141.

60 POLLICINO Y BASSINI, ob. cit., 754.

61 TJUE, *Schrems*, cit., 81.

62 Decisión 2000/520/CE, cit., anexo I, 4, letras a) y b): "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; b) por disposición legal o reglamentaria, o jurisprudencia que originen conflictos de obligaciones o autorizaciones explícitas, siempre que las entidades que recurran a tales autorizaciones puedan demostrar que el incumplimiento de los principios se limita a las medidas necesarias para garantizar los intereses legítimos esenciales contemplados por las mencionadas autorizaciones".

63 TJUE, *Schrems*, cit., 84-86. Véase DE MIGUEL ASENSIO, P. A. Aspectos internacionales de la protección de datos: las sentencias Schrems y Weltimmo del Tribunal de Justicia. *La Ley*

a una evidente injerencia de las autoridades estadounidenses en perjuicio del derecho a la vida privada de los ciudadanos europeos cuyos datos personales se transferían o pudieran transferirse desde la UE a Estados Unidos[64].

El Tribunal estaba consciente que la configuración de una injerencia no vulneraba automáticamente el derecho a la privacidad, ya que este puede ser limitado siempre que se respeten ciertos estándares, tesis que ya se había sostenido en su jurisprudencia anterior[65]. En efecto, de acuerdo al artículo 52.1 CDFUE, las limitaciones a los derechos protegidos en este tratado deben respetar dos estándares centrales: el contenido esencial y el principio de proporcionalidad[66]. Esta norma tiene por objeto advertir que la legitimidad de los límites al ejercicio de los derechos fundamentales dependerá de su sujeción a estos criterios básicos[67].

Es necesario subrayar que en su jurisprudencia anterior sobre datos personales el TJUE no había considerado vulnerado el contenido esencial del derecho a la privacidad. El ejemplo paradigmático es el caso *Digital Rights Ireland*, en que el Tribunal diferenció tácitamente entre los metadatos y el contenido de las comunicaciones, concluyendo que solo el acceso a este último configura una afectación a la esencia del derecho a la privacidad[68]. En palabras sencillas, los metadatos son datos sobre las comunicaciones y pueden referirse a la información personal de los participantes de una comunicación,

Unión Europea, 2015(31), 8, explicando que de esa manera los principios se aplicaban a las empresas autocertificadas, pero sin vincular a las autoridades estadounidenses.

64 TJUE, *Schrems*, cit., 87. Véase RESTA, ob. cit., 714-716. Sobre este punto resulta interesante remitirse a la jurisprudencia del TEDH sobre la noción de injerencia en casos de programas de vigilancia masiva, ya que este Tribunal ha entendido que la mera existencia de una legislación que regule este tipo de programas constituye *per se* una injerencia si se cumplen algunos requisitos. Al respecto, véase TEDH, *Roman Zakharov v. Russia*, application n. 47143/06, judgment, 4 de diciembre de 2015, 164-179.

65 TJUE, *Digital Rights Ireland Ltd. y Minister for Communications*, C-293/12 y C-594/12, 8 de abril de 2014, 38. Véase KOKOTT y SOBOTTA, ob. cit., 223-225. En este caso el Tribunal invalidó una directiva sobre retención de datos personales debido a la vulneración de derechos fundamentales. Se trataba de la *Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE, Diario Oficial de la Unión Europea* L 105/54, 13 de abril de 2006.

66 Art. 52.1 CDFUE: "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. Sólo se podrán introducir limitaciones, respetando el principio de proporcionalidad, 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".

67 Para algunos comentarios generales, véase MANGAS MARTÍN, A. "Artículo 52. Alcance e interpretación de los derechos y principios". En: MANGAS MARTÍN, A. (dir.). *Carta de los Derechos Fundamentales de la Unión Europea. Comentario artículo por artículo*. Bilbao: Fundación BBVA, 2008, 832-837.

68 TJUE, *Digital Rights Ireland*, cit., 39.

al lugar, fecha y hora de emisión de la comunicación, a los sitios web consultados y a otras informaciones relacionadas con la caracterización de las comunicaciones[69]. De todas formas, esta posición no deja de ser polémica, ya que la distinción entre el contenido del mensaje y los metadatos se torna difusa de cara a la protección del derecho a la privacidad, si se tiene en cuenta que la tecnología de vigilancia actual es lo suficientemente invasiva incluso sin el acceso al contenido de las comunicaciones[70]. En nuestra opinión, la recopilación y procesamiento de los metadatos puede vulnerar el contenido esencial de la privacidad, ya que permite "extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado, como los hábitos de la vida cotidiana, los lugares de residencia permanentes o temporales, los desplazamientos diarios u otros, las actividades realizadas, sus relaciones sociales y los medios sociales que frecuentan"[71].

Sin embargo, al no haberse acreditado el acceso al contenido de los datos, *Digital Rights Ireland* concluyó que la infracción del derecho a la privacidad se había producido por el incumplimiento del principio de proporcionalidad. Resumidamente, de acuerdo a la jurisprudencia del TJUE, el test de proporcionalidad en materia de privacidad requiere la satisfacción de tres criterios: 1) que la injerencia persiga una finalidad legítima; 2) que se cumpla el test de idoneidad, esto es, que la injerencia sea adecuada para la consecución de dicha finalidad; y, 3) que se cumpla el test de necesidad, es decir, que la injerencia sea estrictamente necesaria para la consecución de dicha finalidad. En *Digital Rights Ireland* se consideró infringido el último de estos criterios, dado que el sistema de conservación de datos no cumplía con ciertas salvaguardas mínimas, por ejemplo, límites al ámbito de aplicación, la intervención de autoridades nacionales de control, la imposición de un período de tiempo reducido para la conservación de los datos y la posibilidad de ejercicio de un recurso efectivo[72].

Lo llamativo de la sentencia *Schrems* es que el TJUE dio un giro en relación con lo sostenido en la sentencia anterior, al concluir que se había vulnerado

69 Sobre la diferenciación entre datos dinámicos, datos estáticos y metadatos en las comunicaciones, véase MAURER, T. et al. Technological Sovereignty: Missing the Point? An Analysis of European Proposals. Global Public Policy Institute. New America et al., noviembre de 2014. [En línea]. [Consulta: 24 de enero de 2017]. Disponible en: http://www.gppi.net/fileadmin/user_upload/media/pub/2014/Maurer-et-al_2014_Tech-Sovereignty-Europe.pdf, 25-26.

70 Véase Consejo de Derechos Humanos. *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, Frank La Rue*, cit., 15; ACNUDH. *El derecho a la privacidad en la era digital*, cit., 19.

71 TRACOL, X. Legislative Genesis and Judicial Death of a Directive: The European Court of Justice Invalidated the Data Retention Directive (2006/24/EC) thereby Creating a Sustained Period of Legal Uncertainty about the Validity of National Laws which Enacted It. *Computer Law & Security Review*, 2014, 30(6), 741.

72 TJUE, *Digital Rights Ireland*, cit., 45-66. Sobre la aplicación del principio de proporcionalidad en esta sentencia, véase FABBRINI, ob. cit., 79-81; RESTA, ob. cit., 713-714.

el contenido esencial del derecho a la privacidad[73]. En su opinión, "una normativa que permite a las autoridades públicas acceder de forma generalizada al contenido de las comunicaciones electrónicas lesiona el contenido esencial del derecho fundamental al respeto de la vida privada"[74]. Aplicando este criterio a los principios de puerto seguro, en *Schrems* se concluyó que efectivamente constituye una vulneración al contenido esencial, dado 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 de las autoridades públicas a los datos y su utilización posterior a fines específicos, estrictamente limitados y propios para justificar la injerencia que constituyen tanto el acceso a esos datos como su utilización[75].

Esta afirmación es de esencial importancia, porque demuestra que el TJUE consideró que los programas de vigilancia masiva revelados por Snowden eran fidedignos, aunque no se detuvo en reflexionar sobre su soporte probatorio. Además, asumió que programas de esta índole suponen una infracción inaceptable del derecho a la privacidad, asentando un criterio que debería ser aplicado para casos futuros de naturaleza similar y que otros tribunales internacionales deberían tener en cuenta. Finalmente, es destacable que el TJUE, al considerar vulnerado el contenido esencial del derecho a la privacidad haya abandonado el análisis basado en la proporcionalidad[76]. Esta conclusión es reveladora y permite demostrar que a juicio del TJUE dichos programas afectan especialmente la protección de los derechos fundamentales[77].

73 Sobre la diversidad de enfoques entre ambas sentencias, véase POLLICINO Y BASSINI, ob. cit., 762-764; RESTA, ob. cit., 715-716; SCHEININ, M. The Schrems Case. The Essence of Privacy, and Varying Degrees of Intrusion. *Verbassunblog on matters constitutional*, 7 de octubre de 2015. [En línea]. [Consulta: 7 de septiembre de 2016]. Disponible en: http://verfassungsblog.de/the-essence-of-privacy-and-varying-degrees-of-intrusion-2/; URÍA GAVILÁN, ob. cit., 274-276.

74 TJUE, *Schrems*, cit., 94. Véase TJUE. *Digital Rights Ireland*, cit., 39, interpretado *a contrario sensu*.

75 TJUE, *Schrems*, cit., 93.

76 De todas formas, aun aceptando que la seguridad nacional frente a la amenaza terrorista era un fin legítimo para justificar políticas de procesamiento masivo de datos, la sentencia destacó que los programas implementados por Estados Unidos no contemplaban ninguna salvaguarda destinada a restringir la injerencia en la privacidad. Véase TJUE, *Schrems*, cit., 88.

77 URÍA GAVILÁN, ob. cit., 276. De todas formas, no es común que el TJUE realice un análisis diferenciado entre el contenido esencial y la proporcionalidad, tal como se explica en POLLICINO, O. Un *Digital Right to Ptivacy* preso troppo sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel *reasoning* di *Google Spain*. En: RESTA, G. y ZENO-ZENCOVICH, V. *Il diritto all'oblio su internet dopo la sentenza Google Spain*. Roma: Roma Tre-Press, 2015, 13.

4.2. La vulneración del contenido esencial del derecho a la tutela judicial efectiva

La sentencia *Schrems* también consideró que se había vulnerado el contenido esencial del derecho a la tutela judicial efectiva[78]. La jurisprudencia del TJUE ha sido enfática en afirmar que la existencia de un control jurisdiccional efectivo para garantizar el cumplimiento del derecho de la Unión es inherente al Estado de derecho[79]. En el caso que nos ocupa, el derecho interno norteamericano no contemplaba recursos judiciales eficaces para que los ciudadanos europeos pudiesen alegar una vulneración de sus derechos fundamentales en relación con sus datos personales[80], siendo que "[l]a necesidad de disponer de esas garantías es aún más importante cuando los datos personales se someten a un tratamiento automático y existe un riesgo elevado de acceso ilícito a ellos"[81]. Por tanto, el contenido esencial del derecho a la tutela judicial efectiva resultaba evidentemente vulnerado[82]. Por lo demás, la aplicación del derecho comunitario no puede impedir el ejercicio de la tutela judicial efectiva, que en materia de datos personales se concreta acudiendo a las autoridades nacionales de control[83].

CONCLUSIONES

En un contexto en el que el acuciante problema del terrorismo internacional ha desequilibrado la balanza en favor de la seguridad nacional por sobre los derechos fundamentales, la decisión del TJUE en el caso *Schrems* viene a establecer barreras que los Estados no pueden traspasar en materia de protección de la privacidad. En este sentido, si bien el TJUE no discute que la

78 López Escudero, M. Artículo 47. Derecho a la tutela judicial efectiva y a un juez imparcial. En: Mangas Martín (dir.). *Carta de los Derechos Fundamentales de la Unión Europea*, cit., 739-758.

79 TJUE, *Schrems*, cit., 95. Véase TJUE, *UGT-Rioja y otros*, C-428/06 a C-434/06, 11 de septiembre de 2008, 80; TJUE, *Union Nationale des Entraineurs et Cadres Techniques Professionnels du Football (UNECTEF) contra Georges Heylens y otros*, Asunto 222/86, 5 de octubre de 1987, 14.

80 TJUE, *Schrems*, cit., 89. Al respecto cabe señalar que los únicos medios de reclamación existentes en Estados Unidos eran algunos mecanismos de arbitraje privado y la intervención de la Comisión Federal de Comercio, pero el ámbito de aplicación de estas medidas estaba acotado al uso comercial de los datos personales, siendo imposible utilizarlas para reclamar la vulneración de derechos fundamentales frente a actividades de vigilancia. En relación con este punto, véase TJUE. *Conclusiones del Abogado General, Sr. Yves Bot*, 204-207; Tracol. 'Invalidator' Strikes Back, cit., 348.

81 TJUE, *Schrems*, cit., 91. Véase TJUE, *Digital Rights Ireland*, cit., 54-55. En el mismo sentido se ha pronunciado el TEDH: *Klass and others v. Germany*, application n. 5029/71, judgment, 6 de septiembre de 1978, 55; *Rotaru v. Romania*, application n. 28341/95, judgment, 4 de mayo de 2000, 59.

82 TJUE, *Schrems*, cit., 95.

83 Véase Pollicino y Bassini, ob. cit., 748-750; López Escudero, ob. cit., 743 ss.

recopilación, procesamiento y conservación de datos personales para prevenir actos terroristas u otros delitos puede ser un fin legítimo para restringir la privacidad, deja claro que cualquier normativa que autorice el acceso generalizado a los datos personales sin establecer ninguna salvaguarda vulnera el contenido esencial del derecho a la privacidad, tal como ocurría con los programas de vigilancia masiva que estaban desarrollando algunos Estados tras los atentados del 11 de septiembre. Con esta posición, el TJUE da un giro en su jurisprudencia y abandona el análisis basado en la proporcionalidad que había utilizado en sentencias anteriores, marcando un hito en pos de la defensa del derecho a la privacidad. A su vez, el TJUE concluye que no contar con garantías eficaces a las que los ciudadanos puedan acudir cuando consideren vulnerados sus derechos fundamentales en relación con sus datos personales infringe el derecho a la tutela judicial efectiva y determina que el derecho comunitario tampoco puede impedir el ejercicio de la misma, que en materia de protección de datos personales se concreta acudiendo a las autoridades nacionales de control.

A partir del caso *Schrems*, el TJUE no solo se pone a la vanguardia en la protección de los datos personales, allanando el camino para casos de similar naturaleza, sino que también reafirma el control de los ciudadanos europeos sobre sus propios datos al establecer la obligación de las autoridades nacionales de control de examinar cualquier reclamación relativa al tratamiento de sus datos personales por parte de otros Estados. Asimismo, asevera la facultad de estas autoridades de suspender cualquier transferencia de datos cuando estos Estados no cumplen con un estándar adecuado de protección. Sin duda, con esta decisión el TJUE, por un lado, refuerza la idea de la independencia de las autoridades de control que ya venía manteniendo en su jurisprudencia anterior y, por otro, consolida el papel de las mismas como máximos guardianes de los derechos fundamentales en lo que respecta al tratamiento de datos personales.

En esta era digital con enormes desafíos por delante, la sentencia *Schrems* se configura como un caso histórico en la defensa del derecho a la privacidad. No obstante, los tribunales nacionales e internacionales tendrán que afrontar en el futuro numerosos interrogantes. Solo cabe mencionar algunos ejemplos a modo de desafíos pendientes. Uno de los dilemas más relevantes dice relación con la aplicabilidad extraterritorial de los tratados de derechos humanos. En efecto, estos tratados obligan a los Estados parte en relación con las personas que se encuentren bajo su jurisdicción, configurando una excepción al principio de territorialidad de los tratados. Sin embargo, adaptar la regla de la extraterritorialidad al contexto digital es un problema de difícil solución ante el cual se están barajando respuestas diversas. Un segundo desafío consiste en defender la tesis de la prohibición de las diferencias discriminatorias entre nacionales y extranjeros ante la protección brindada por el derecho a la privacidad. El argumento según el cual la protección de un

ordenamiento jurídico nacional sobre la privacidad alcanzaría solamente a los nacionales tensiona insoportablemente el principio de igualdad erigiendo una distinción arbitraria entre nacionales y extranjeros, ubicando a estos últimos en un limbo de absoluta desprotección ante las técnicas de vigilancia transfronteriza en contextos digitales.

Por su parte, la participación de las empresas en las técnicas de vigilancia, principalmente, proporcionando a los Estados un acceso poco restringido y carente de controles adecuados sobre los datos personales de los usuarios, plantea la necesidad de discutir si es plausible obligar internacionalmente a los agentes no estatales al respeto y garantía de los derechos fundamentales. Si bien este tópico ya está siendo abordado, es indispensable centrar la mirada en las peculiaridades que plantean los contextos digitales. Finalmente, es necesario clarificar la operatividad de los estándares que habilitan las injerencias a la privacidad de las personas en el marco de contextos sensibles como los planteados por la lucha contra el terrorismo. Esta tarea debe llevarse a cabo teniendo presente que el discurso de los derechos humanos es especialmente valioso para la búsqueda de respuestas sensatas y racionales.

REFERENCIAS

Doctrina

Álvarez Caro, M. y Recio Gayo, M. (2015). Hacia un acuerdo Safe Harbor renovado para la transferencia internacional de datos entre EE.UU y la UE. *Papeles de Derecho Europeo e Integración Regional* [En línea]. Madrid, IDEIR, n.º 25. [Consulta: 25 de enero de 2017]. Disponible en: https://www.ucm.es/data/cont/docs/595-2015-06-15-Binder218.pdf.

Bowden, C. (2013). *The US Surveillance Programmes and their Impact on EU Citizens' Fundamental Rights*. Brussels: European Parliament - Directorate-General for Internal Policies.

Cole, D. (2014). The Three Leakers and what to do about them. *The New York Review of Books* [En línea], 6 de febrero. Vol. 61(2). [Consulta: 16 de enero de 2017]. Disponible en: http://www.nybooks.com/articles/2014/02/06/three-leakers-and-what-do-about-them/.

Comella, C. (2015). Alcune considerazioni sugli aspetti tecnologici della sorveglianza di massa, a margine della sentenza "Safe Harbor" della Corte di Giustizia dell' Unione Europea. *Diritto dell'informazione e dell'informatica*. Vol. 31(4-5), 719-740.

Darcy, S. (2015). Battling for the Rights to Privacy and Data Protection in the Irish Courts. *Utrecht Journal of International and European Law*. Vol. 31(80), 131-136.

De Miguel Asensio, P. A. (2015). Aspectos internacionales de la protección de datos: las sentencias Schrems y Weltimmo del Tribunal de Justicia. *La Ley Unión Europea*. (31), 1-10.

Díaz Díaz, E. (2016). "El nuevo Reglamento General de Protección de Datos de la Unión Europea y sus consecuencias jurídicas para las instituciones. *Revista Aranzadi Doctrinal*. (6), 155-190.

Eckes, C. y Abazi, V. (2015). Safe Harbor Case: Safeguarding European Fundamental Rights or Creating a Patchwork of National Data Protection? *UK Constitutional Law Blog* [En línea], 9 de octubre. [Consulta: 29 de septiembre de 2016]. Disponible en: https://ukconstitutionallaw.org/2015/10/09/christina-eckes-and-vigjilenca-abazi-safe-harbour-case-safeguarding-european-fundamental-rights-or-creating-a-patchwork-of-national-data-protection/

Fabbrini, F. (2015). Human Rights in the Digital Age: The European Court of Human Rights in the Data Retention Case and its Lessons for Privacy and Surveillance in the United States. *Human Rights in the Digital Age*. (28), 65-95.

Falchetta, T. (2016). How to Bridge the Gap? Corporate and Government Surveillance Examined at the UN. *ejil: Talk!* [En línea]. 7 de diciembre. [Consulta: 27 de enero de 2017]. Disponible en: http://www.ejiltalk.org/how-to-bridge-the-gap-corporate-and-government-surveillance-examined-at-the-un/#more-14808

Finocchiaro, G. (2015). La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems. *Diritto dell'informazione e dell'informatica*. 31(4-5), 779-799.

Gryffroy, P. (2016). Taking a Look at Two Cases in the Margin of the cjeu's 'Privacy Spring', before and after the General data Protection Regulation: Weltimmo and Bara. *Jean-Monnet-Saar/Europarecht online*. [En línea]. 21 de junio. [Consulta: 16 de enero de 2017]. Disponible en: http://jean-monnet-saar.eu/?p=1453.

Kokott, J. y Sobotta, C. (2013). The Distinction between Privacy and Data Protection in the Jurisprudence of the cjeu and the ECtHR. *International Data Privacy Law*. 3(4), 222-228.

López Escudero, M. (2008). Artículo 47. Derecho a la tutela judicial efectiva y a un juez imparcial. En: Mangas Martín, A. (dir.). *Carta de los Derechos Fundamentales de la Unión Europea*. *Comentario artículo por artículo*. Bilbao: Fundación bbva, 739-758.

Mangas Martín, A. (2008). Artículo 52. Alcance e interpretación de los derechos y principios. En: Mangas Martín, A. (dir.). *Carta de los Derechos Fundamentales de la Unión Europea*. *Comentario artículo por artículo*. Bilbao, Fundación bbva, 826-851.

Margulies, P. (2014). The nsa in Global Perspective: Surveillance, Human Rights and International Counterterrorism. *Fordham Law Review*, 82(5), 2137-2167.

Maurer, T. et al. (2014). Technological Sovereignty: Missing the Point? An Analysis of European Proposals. En *Global Public Policy Institute*. [En línea]. New America et al., noviembre. [Consulta: 24 de enero de 2017]. Disponible en: http://www.gppi.net/fileadmin/user_upload/media/pub/2014/Maurer-et-al_2014_Tech-Sovereignty-Europe.pdf

Milanovic, M. (2015). Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age. *Harvard International Law Journal*. Winter, 56(1), 81-146.

Resta, G. (2015). La sorveglianza elettronica di massa e il conflitto regolatorio usa/ue. *Diritto dell'informazione e dell'informatica*. 31(4-5), 697-718.

Peers, S. (2015). The Party's Over: EU Data Protection Law after the Schrems Safe Harbor Judgment. *EU Law Analysis*. [En línea]. 7 de octubre. [Consulta: 16 de enero de 2017]. Disponible en: http://eulawanalysis.blogspot.cl/2015/10/the-partys-over-eu-data-protection-law.html

Piroddi, P. (2015). I trasferimenti di dati personali verso paesi terzi dopo la sentenza Schrems e nel nuovo regolamento generale sulla protezione dati. *Diritto dell'informazione e dell'informatica*. 31(4-5), 827-864.

Pollicino, O. (2015). Un *Digital Right to Ptivacy* preso troppo sul serio dai giudici di Lussemburgo? Il ruolo degli artt. 7 e 8 della Carta di Nizza nel *reasoning* di *Google Spain*. En: Resta, G. y Zeno-Zencovich, V. *Il diritto all'oblio su internet dopo la sentenza Google Spain*. Roma: Roma Tre-Press, 7-28.

Pollicino, O. y Bassini, M. (2015). La Carta dei Diritti Fondamentali dell' Unione Europea nel reasoning dei giudici di Lussemburgo. *Diritto dell'informazione e dell'informatica*. 31(4-5), 741-777.

Resta, G. (2015). La sorveglianza elettronica di massa e il conflitto regolatorio usa/ue. *Diritto dell'informazione e dell'informatica*. 31(4-5), 697-718.

Sarmiento, D. (2015). What Schrems, Delvigne and Celaj Tell us about the State of Fundamental Rights in the EU. *Despite our differences Blog*. [En línea]. 16 de octubre. [Consulta: 8 de septiembre de 2016]. Disponible en: https://despiteourdifferencesblog.wordpress.com/2015/10/16/what-schrems-delvigne-and-celaj-tell-us-about-the-state-of-fundamental-rights-in-the-eu/

Scheinin, M. (2015). The Schrems Case. The Essence of Privacy, and Varying Degrees of Intrusion. *Verbassunblog on matters constitutional*. [En línea]. 7 de octubre. [Consulta: 7 de septiembre de 2016]. Disponible en: http://verfassungsblog.de/the-essence-of-privacy-and-varying-degrees-of-intrusion-2/

Škrinjar, M. (2015). Schrems v Data Protecion Commissioner (Case C-362/14): Empowering National Data Protection Authorities. *Croatian Yearbook of European Law and Policy*. (11), 259-275.

Tracol, X. (2016). "Invalidator" Strikes Back: the Harbor has Never Been Safe. *Computer Law & Security Review*. 32(2), 345-362.

Tracol, X. (2014). Legislative Genesis and Judicial Death of a Directive: The European Court of Justice Invalidated the Data Retention Directive (2006/24/EC) thereby Creating a Sustained Period of Legal Uncertainty about the Validity of National Laws which Enacted It. *Computer Law & Security Review*. 30(6), 736-746.

Uría Gavilán, E. (2016). 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*. *Revista de Derecho Comunitario Europeo*. Enero/abril, (53), 261-282.

Woods, L. (2015). Data Protection: the CJEU Clarifies the Applicable Law and Jurisdiction. *EU Law Analysis* [En línea], 13 de octubre. [Consulta: 24 de enero de 2017]. Disponible en: http://eulawanalysis.blogspot.cl/2015/10/data-protection-cjeu-clarifies.html

Jurisprudencia

Alta Corte de Irlanda (High Court). *Schrems v. Data Protection Commissioner* [2014] IEHC 213.

Tribunal Europeo de Derechos Humanos. *Big Brother Watch v. United Kingdom*, Communicated Case, application n.º 58170/13, 2013.

Tribunal Europeo de Derechos Humanos. *Klass and others v. Germany*, application no. 5029/71, judgment, 6 de septiembre de 1978.

Tribunal Europeo de Derechos Humanos. *Rotaru v. Romania*, application no. 28341/95, judgment, 4 de mayo de 2000.

Tribunal Europeo de Derechos Humanos. *Roman Zakharov v. Russia*, application no. 47143/06, judgment, 4 de diciembre de 2015.

Tribunal de Justicia de la Unión Europea. *Comisión Europea, Reino Unido de Gran Bretaña, Irlanda del Norte y Consejo de la Unión Europea v. Yassin Abdullah Kadi*, C-584/10 P, C-593/10 P y C-595/10 P, 18 de julio de 2013.

Tribunal de Justicia de la Unión Europea. *Comisión Europea v. Hungría*, C- 288/12, 8 de abril 2014.

Tribunal de Justicia de la Unión Europea. *Comisión Europea v. República de Austria*, C- 614/10, 16 de octubre de 2012.

Tribunal de Justicia de la Unión Europea. *Comisión Europea v. República Federal de Alemania*, C-518/07, 9 de marzo de 2010

Tribunal de Justicia de la Unión Europea. *Conclusiones del Abogado General, Sr. Yves Bot*, Asunto C-362/14, 23 de septiembre de 2015.

Tribunal de Justicia de la Unión Europea. *Digital Rights Ireland Ltd y Minister for Communications*, C-293/12 y C-594/12, 8 de abril de 2014.

Tribunal de Justicia de la Unión Europea. *Kadi v. Consejo y Comisión*, T-315/01, 21 de septiembre de 2005.

Tribunal de Justicia de la Unión Europea. *Maximilian Schrems y Data Protection Commissioner*, C-362/14, 6 de octubre de 2015.

Tribunal de Justicia de la Unión Europea. *UGT-Rioja y otros*, C-428/06 a C- 434/06, 11 de septiembre de 2008.

Tribunal de Justicia de la Unión Europea. *Union Nationale des Entraineurs et Cadres Techniques Professionnels du Football (UNECTEF) c. Georges Heylens y otros***,** Asunto 222/86, 5 de octubre de 1987.

Tribunal de Justicia de la Unión Europea. *Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság*, C-230/14, 1 de octubre de 2015.

Tribunal de Justicia de la Unión Europea. *Yassin Abdullah Kadi v. Comisión Europea*, T-85/09, 30 de septiembre de 2010.

Tribunal de Justicia de la Unión Europea. *Yassin Abdullah Kadi y Al Barakaat International Foundation v. Consejo de la Unión Europea y Comisión de las Comunidades Europeas*, C-402/05 P y C-415/05 P, 3 de septiembre de 2008.

Instrumentos internacionales

Alto Comisionado de Naciones Unidas para los Derechos Humanos. *El derecho a la privacidad en la era digital*. A/hrc/27/37, 30 de junio de 2014.

Asamblea General de Naciones Unidas. *El derecho a la privacidad en la era digital*, Res. 68/167, 18 de diciembre de 2013.

Asamblea General de Naciones Unidas. *El derecho a la privacidad en la era digital*, Res. 69/166, 18 de diciembre de 2014.

Asamblea General de Naciones Unidas, *El derecho a la privacidad en la era digital*, A/C.3/71/L.39/Rev.1, 16 de noviembre de 2016

Comisión Europea. *Comunicación al Parlamento Europeo y al Consejo. Restablecer la confianza en los flujos de datos entre la UE y ee.uu.* com(2013) 846 final, 27 de noviembre de 2013.

Comisión Europea. *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, 27 de noviembre de 2013.

Comisión Europea. *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*, *Diario Oficial de las Comunidades Europeas*, n.º 125, 25 de agosto de 2000. Unión Europea. *Carta de los Derechos Fundamentales de la unión Europea*. (2016/C 202/02), versión consolidada, *Diario Oficial de la Unión Europea*, C 202/1, 17 de junio de 2016.

Consejo de Derechos Humanos. *Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, Frank La Rue*. A/hrc/23/40, 17 de abril de 2013.

Consejo de Derechos Humanos. *Informe del Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo, Martin Scheinin*. A/hrc/13/37, 28 de diciembre de 2009.

Consejo de Derechos Humanos. *Informe de Martin Scheinin, Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo*. A/hrc/14/46, 17 de mayo de 2010.

Comisión Interamericana de Derechos Humanos-Relatoría Especial para la Libertad de Expresión. *Libertad de expresión e Internet*. oea/Ser.L/V/II, cidh/rele/inf. 11/13, 31 de diciembre de 2013; Relator Especial de las Naciones Unidas (onu) para la Libertad de Opinión y de Expresión et al. *Declaración conjunta sobre libertad de expresión e internet*. En: *oea* [En Línea], 1 de junio de 2011. [Consulta: 31 de enero de 2017]. Disponible en: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=849&lID=2

Relator Especial de las Naciones Unidas (onu) para la Libertad de Opinión y de Expresión et al. *Declaración conjunta sobre la libertad de expresión y las respuestas a las situaciones de conflicto*. En *oea* [En Línea], 4 de mayo de 2015. [Consulta: 31 de enero de 2017]. Disponible en: http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=987&lID=2

Relator Especial de las Naciones Unidas (onu) para la Libertad de Opinión y de Expresión et al. *Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión*. En *oea* [En Línea], 2 de junio de 2013. [Consulta: 31 de enero de 2017]. Disponible en: http://www.oas.org/ES/cidh/expresion/showarticle.asp?artid=926&LID=2

Relatoría Especial para la Libertad de Expresión et al. *Declaración conjunta sobre Wikileaks*. En *oea* [En Línea], 21 de diciembre de 2010. [Consulta: 31 de enero de 2017]. Disponible en: http://www.oas.org/ES/cidh/expresion/showarticle.asp?artid=889&LID=2

Unión Europea. *Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos*, *Diario Oficial de las Comunidades Europeas*, L281, 23 de noviembre de 1995.

Unión Europea. *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*, *Diario Oficial de la Unión Europea*, L105/54, 13 de abril de 2006.

Unión Europea. *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos que viene a derogar y sustituir a la Directiva 95/46/CE*, *Diario Oficial de la Unión Europea*, L119, 4 de mayo de 2016.

Unión Europea. *Tratado de Funcionamiento de la Unión Europea*. (2016/C 202/01), versión consolidada, *Diario Oficial de la Unión Europea*, C202/2, 17 de junio de 2016.