LA PROTECCION DE DATOS PERSONALES EN LA MÁS RECIENTE JURISPRUDENCIA DEL TJUE: LOS DERECHOS DE LA CDFUE COMO PARÁMETRO DE VALIDEZ DEL DERECHO EUROPEO, Y SU IMPACTO EN LA RELACIÓN TRANSATLÁNTICA UE-EUUU

JUAN FERNANDO LÓPEZ AGUILAR
Catedrático de Derecho Constitucional
Universidad de las Palmas de Gran Canaria

SUMARIO

I. Introducción: la constitucionalización de la protección de datos personales tras el Tratado de Lisboa. II. La protección de datos personales en la relación transatlántica. El «escudo de privacidad» UE-EE.UU (*EU-US privacy shield*). La protección de datos en el llamado *Umbrella Agreement* UE-EE.UU. III. Dos relevantes sentencias del TJUE con impacto en la relación transatlántica: la sentencia del TJ de 8 de abril de 2014 (*Caso Digital Rights Ireland)* y la sentencia del TJ de 6 de octubre de 2015 (*Caso Schrems*): los derechos fundamentales de la Carta de Derechos de la UE como parámetro de validez del Derecho europeo. IV. Conclusiones.

I. INTRODUCCIÓN: LA CONSTITUCIONALIZACIÓN DE LA PROTECCIÓN DE DATOS PERSONALES TRAS EL TRATADO DE LISBOA

Es comúnmente aceptado que el Tratado de Lisboa (en adelante, TL) cristaliza un prolongado esfuerzo por revestir la construcción europea de dimensión constitucional. Tanto por la incorporación al Tratado de la UE, según fue refundido por el TL (y en adelante TUE) de pronunciamientos explícitos (arts. 2, 3, 4 y 6 TUE) acerca de la fuerza vinculante de los *principios generales* y de las *tradiciones constitucionales comunes* de los Estados miembros (en adelante, EEMM) como fuente del Derecho europeo, como por la recepción del acervo jurisprudencial del Tribunal de Justicia (TJUE) de Luxemburgo acerca de los parámetros en materia de

Derechos Humanos y Derechos Fundamentales del Tribunal Europeo de Derechos Humanos (TEDH) de Estrasburgo sobre la base del Convenio de Roma de 1950 y sus Protocolos anexos (en adelante, CEDH), cuya ratificación y adhesión por la UE se establece como mandato taxativo en el propio art. 6.2 TUE[1].

Pero, sobre todo, también, por la incorporación, al fin, de un genuino *Bill of Rights*, la Carta de Derechos Fundamentales de la UE[2] (CDFUE) con el «mismo valor jurídico que los Tratados» (art. 6.1 TUE)[3].

Precisamente esta decantación acerca del valor vinculante de los derechos de la Carta debe mucho a la jurisprudencia del TJ, que, como se cita reiteradamente en todos los escritos sobre la materia, arranca en el *caso Stauder* (1969)[4] que efectúa un recorrido en que las sentencias *Internationale Handelsgesellschaft* (1970)[5], *Nold* (1974)[6], *Les Verts* (1986)[7], entre otras de usual colación en doctrina, señalan el punto de despegue de la formalización de los derechos como parámetro de validez del Derecho derivado de la Unión. Canon, pues, de validez de un sistema de Derecho que, conforme a los principios de primacía, eficacia directa, unidad del ordenamiento jurídico europeo e interpretación uniforme garantizada por el TJ, va a proyectarse también sobre el Derecho nacional (los ordenamientos propios) de los EE.MM «cuando apliquen derecho de la UE (arts. 51 a 53 CDFUE)», puesto que la garantía de la primacía europea está en todo caso sometida a una lectura expansiva por parte del propio TJ[8].

1 Cfr. a este respecto, por todos, algunos escritos hoy clásicos: Rubio Llorente, F.: «El constitucionalismo de los Estados integrados de Europa», *Revista Española de Derecho Constitucional (REDC)* Madrid: Centro de Estudios Políticos Constitucionales, 48, 1996; Saiz Arnaiz, A.: *La apertura constitucional al Derecho Internacional y Europeo de los Derechos Humanos. El art. 10.2 de la Constitución Española,* Consejo General del Poder Judicial, Madrid, 1999; Rodríguez Iglesias, G. C. y Valle Gálvez, A.: «El Derecho comunitario y las relaciones entre el Tribunal de Justicia de las Comunidades Europeas, el Tribunal Europeo de Derechos Humanos y los Tribunales Constitucionales nacionales», *Revista de Derecho Comunitario,* n.º 2, Madrid, Julio/Diciembre 1997; Weiler, J.H.H.: *Europa, fin de siglo*, Madrid, Centro de Estudios Políticos y Constitucionales, 1995; Balaguer Callejón, F., «Constitucionalismo Multinivel y Derechos Fundamentales en la Unión Europea», en AA.VV., *Teoría y metodología del Derecho. Estudios en Homenaje al Profesor Gregorio Peces-Barba*, Vol. II, Dykinson, Madrid, 2008, pp. 133-157; «Fuentes del derecho, espacios constitucionales y ordenamientos jurídicos», *Revista Española de Derecho Constitucional*, n.º 69, 2003, pp. 181-213; y Cámara Villar, G., «Los derechos fundamentales en el proceso histórico de construcción de la Unión Europea y su valor en el Tratado constitucional», *ReDCE*, n.º 4, Julio-Diciembre, 2005, pp. 9-42. Dirección electrónica: http://www.ugr.es/~redce/REDCE4/articulos/01camara.htm.

2 Proclamado por el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión Europea el 7 de diciembre de 2000 en Niza. Una versión revisada de la Carta fue proclamada y firmada el 12 de diciembre de 2007 en Estrasburgo igualmente por el Parlamento Europeo, la Comisión Europea y el Consejo.

3 Véase por todos, Rolla, G., «La Carta de Derechos Fundamentales de la Unión Europea y el Convenio Europeo de los Derechos Humanos y de las Libertades Fundamentales: su contribución a la formación de una jurisdicción constitucional de los derechos y las libertades», *Revista europea de derechos fundamentales,* n.º 15, 2010, pp. 15-39.

4 Asunto *STAUDER v. Stadt Ulm — Sozialamt* (29/69), de 12 de noviembre de 1969.

5 Asunto *Internationale Handelsgesellschaft mbH* (11/70), de 17 de diciembre de 1970.

6 Asunto *Nold* (4/73), de 14 de mayo de 1974.

7 Asunto *Partido Ecologista Les Verts v. Parlamento Europeo* (294/83), de 23 de abril de 1986.

8 Por todos, vid. Diez-Picazo, L. M.: Díez-Picazo, *Constitucionalismo de la Unión Europea*, Madrid: Civitas, 2002.

La tarea jurisdiccional del TJUE ha condicionado así, intensamente, el desenvolvimiento histórico del «diálogo entre ordenamientos» y «diálogo entre tribunales», lo que comporta interacciones dialogales y dinámicas entre derechos consignados en la CDFUE (asegurada por el TJ), derechos del CEDH (protegido por el TEDH) y derechos fundamentales de las Constituciones de los EE.MM (Tribunales Constitucionales y poderes judiciales nacionales). Se delinea así el perímetro dinámico de un «diálogo entre Tribunales» que alimenta la cultura de un *Derecho Común* europeo[9].

Los estudios más recientes de la doctrina especializada señalan al menos tres ámbitos específicos de incidencia decisiva de la jurisprudencia del TJ sobre la de los tribunales garantes de los ordenamientos de los EEMM: el acceso a la Justicia y a la tutela judicial; la igualdad de trato y no discriminación; y, en lo que nos ocupa, privacidad, vida privada y protección de datos.

En efecto, la protección de datos se encuadra en la consagración de los derechos a la intimidad y a la vida privada (arts. 7 y 8 CDFUE), en combinación con el derecho a la tutela judicial (art. 47 CDFUE). Se corresponde una elaboración actualizada y extensa de los derechos reconocidos en el art. 18 CE; al honor (a la reputación) y a la propia imagen y derecho a la intimidad personal, familiar; a la inviolabilidad del domicilio y de las comunicaciones (por cualquier medio o tecnología disponible)… y el mandato constitucional español que ordena la «limitación» del tratamiento de datos para mejor la garantía de los derechos relativos a la privacidad (derechos «personalísimos», o de la personalidad).[10]

Así, con lexicología imperfecta, el art. 18.4 CE establece: «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno uso de sus derechos». Parece claro que ya en 1978 (fecha temprana, a la vista de la revolución tecnológica e informacional que en tiempo mucho más reciente, aunque vertiginoso, nos ha conducido al horizonte de la digitalización de la sociedad en red), el constituyente advierte de la relevancia constitucional de acotar el potencial uso de las aplicaciones informáticas para asegurar los derechos de la personalidad en la denominada —desde el pionero ensayo de Pablo Lucas Murillo de la Cueva— «autodeterminación informativa»[11].

9 Cfr. Alonso Garcia, R.: *Derecho comunitario, derecho nacionales y derecho común europeo*, Madrid, Editorial Civitas S.A., 1989; Sáiz Arnaiz, A., «El Tribunal de Justicia, los Tribunales Constitucionales y la tutela de los derechos fundamentales en la Unión Europea: entre el (potencial) conflicto y la (deseable) armonización: de los principios no escritos al catálogo constitucional, de la autoridad judicial a la normativa», en Gómez Fernández, I. (coord.)/Cartabia, M. (dir.)/De Witte, B. (dir.)/Pérez Tremps, P. (dir.), *Constitución europea y constituciones nacionales*, Tirant lo Blanch, Valencia, 2005, pp. 531-588; y Carmona Contreras, A.: «El espacio europeo de los derechos fundamentales: de la Carta a las constituciones nacionales», *Revista Española de Derecho Constitucional*, n.º 107, pp. 13-40, Madrid, 2016.

10 Vid. Aguado Renedo, C.: «La protección de los datos personales ante el Tribunal Constitucional español», *Revista Mexicana de Derecho Constitucional,* n.º 23, julio-diciembre 2010, pp. 3-25.

11 Véase Lucas Murillo de la Cueva, P.: *El derecho a la autodeterminación informativa*, Tecnos, Temas clave, Madrid, 1990.

Referentes de este encuadre lo han sido durante este tiempo tanto el art. 8 CEDH y el *Convenio del Consejo de Europa sobre Protección de Datos Personales* (Convenio 108/81)[12] como la Directiva UE 95/46[13] y los arts. 7 y 8 CDFUE en el TL. Pues bien, en el marco de esas coordenadas, en el Derecho español han sido dos las Leyes Orgánicas que han jalonado el historial de desarrollo del art. 18.4 CE: la llamada LORTAD (LO 5/92, de 29 de octubre[14]) y la posterior LOPD (LO 15/99, de 13 de diciembre[15]). Sobre el título competencial del art. 149.1.1CE, la LOPD instituyó la Agencia Española de Protección de Datos[16] (autoridad nacional de supervisión, en la terminología europea) para controlar la creación y uso de ficheros automáticos por parte de poderes públicos y empresas y particulares. A partir de estos mimbres, y en una sucesión de casos en los que se enjuiciaba la constitucionalidad de las disposiciones legales, la jurisprudencia constitucional del TC estableció con claridad que el derecho reconocido en el art. 18.4 CE es un «derecho autónomo» (la «libertad frente a potenciales agresiones a la dignidad y a la libertad proveniente del uso ilegítimo de otras amenazas» (STC 254/93[17]), por el que se protege la totalidad de los datos de carácter personal, no sólo de los materialmente calificables como «íntimos» (art. 18.1 CE)[18]. Son, pues, *todos los datos* de la personalidad (STC 292/2000[19]), e independientemente de la ciudadanía española o la condición de extranjero. Por su parte, la jurisprudencia del TEDH viene a consolidarse en el *Asunto Rotaru c. Rumanía* (4 de mayo de 2000): de acuerdo con la doctrina de esta resolución, el art. 8 CEDH impone límites a la recogida y tratamiento de datos, robusteciendo la posibilidad de rectificación de su utilización abusiva (*Amman c. Suiza,* de 16 de febrero 2000, y *Z. contra Finlandia*, de 25 de febrero 1997). En esa jurisprudencia se perfilan a menudo las aplicaciones concretas de los principios constitucionales de relevancia indubitada

12 Convenio 108 del Consejo de Europa, de 28 de enero de 1981, sobre protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, ratificado por España y publicado en el *Boletín Oficial del Estado* n.º 274, de 15 de noviembre de 1985.

13 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.

14 Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal (Vigente hasta el 14 de enero de 2000).

15 Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

16 Real Decreto 428/1993, de 26 de marzo, por el que se aprueba el Estatuto de la Agencia de Protección de Datos (AEPD).

17 Sentencia de 20 de julio de 1993 que resuelve el recurso de amparo n.º 1827/90, a la que el magistrado Miguel Rodríguez-Pinero y Bravo-Ferrer formula un voto particular. Su ponente es el magistrado Fernando García-Mon y González Regueral.

18 Véase Villaverde Menéndez I., «Protección de datos personales, derecho a ser informado y autodeterminación informativa del individuo. A propósito de la STC 245/1993», *Revista Española de Derecho Constitucional,* n.º 41, 1994, pp. 187 y ss.

19 Sentencia 292/2000, de 30 de noviembre de 2000 del Tribunal Constitucional. Recurso de inconstitucionalidad respecto de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

como la reserva de Ley y los criterios de necesidad y de proporcionalidad como sustrato de la licitud del tratamiento de datos, en conjugación con el principio de la finalidad legítima del tratamiento de datos y, en su caso, del acceso (*Gaskin c. Reino Unido*, 7 de julio 1989)[20].

Esta elaboración previa es sintetizada con especial acierto en la posterior CDFUE (arts. 7 y 8, en su lectura sistemática con los arts. 51 a 54 CDFUE, sobre reglas de aplicación). Si bien la jurisprudencia constitucional del TC ya había establecido en España la afirmación del derecho de acceso y cancelación de los contenido ilícitos (véanse las SSTC 11/98, de 13 de enero, 202/99, de 08 de noviembre, o 290/2000, de 30 de noviembre), va a ser el Derecho europeo el que va a cristalizar un singular refuerzo al derecho de cancelación en lo que se conoce como «derecho al olvido» (del «*Right to be let alone*», que teorizó J. Brandeis al «*Right to be forgotten*», en alemán «*Recht auf Vergessen*»)[21].

Pues bien, a partir de ahí, coincido con quienes subrayan que, en la jurisprudencia del TJUE acerca de los derechos consignados en la CDFUE, seguramente es a propósito de la protección de datos (en el marco de la consagración de los derechos a la vida privada y de privacidad) en donde su influencia ha sido más determinante para los TC nacionales y los poderes judiciales de los EEMM. En efecto, el TJUE ha venido estableciendo en estos últimos años una jurisprudencia, en su conjunto, sólida e incisiva. En modo que, recientemente, interpretando los derechos de los arts. 7 y 8 CDFUE, con una aproximación asertiva y decididamente favorable a la garantía de la privacidad y a los principios europeos de reserva de Ley de *necesidad* y de *proporcionalidad* y *legitimidad* de la finalidad (*purpose limitation*) junto a la delimitación temporal de la retención y conservación de datos (*retention period*). Y ello tanto en los asuntos (*Case Law*) concernientes a la trasposición de la Directiva de Protección de Datos 95/46 en el Derecho interno, como en los relativos a la aplicación del Derecho de los EEMM.

Así lo indica el examen de la cuestión prejudicial elevada ante el TJUE por el Tribunal Supremo de España (TS) en el *Asunto Asnef*[22]. La transposición de la Directiva 95/46 (efectuada en su día por LO 15/99) marca la ocasión de contraste entre el refuerzo de la intimidad y el acceso a los datos personales en el Derecho europeo, particularmente a la luz de la doctrina armonizadora del TJUE, y los denominados «márgenes de apreciación» de los EE.MM. Pero posiblemente el

20 Seguimos, en este punto, la explicación de Díez-Picazo, L. M.: *Sistema de derechos fundamentales,* Madrid, Thomson, Civitas, 2005, pp. 277 y ss.

21 Véase sobre este extremo Rallo Lombarte, A.: *El derecho al olvido en internet: Google versus España*, Centro de Estudios Políticos y Constitucionales, Madrid, 2014.

22 Asunto C-238/05, por el que el TS eleva una petición de cuestión prejudicial, que exige la interpretación del artículo 81 TCE, en el asunto entre ASNEF-EQUIFAX, Servicios de Información sobre Solvencia y Crédito, S.L. y la Administración del Estado contra la Asociación de Usuarios de Servicios Bancarios (AUSBANC), suscitado por un registro o sistema de intercambio de información entre entidades financieras sobre la solvencia de los clientes. Asunto resuelto por la sentencia del TJCE de 23 de noviembre de 2006.

caso más relevante en la secuencia más reciente lo fija el *Asunto Google Spain*[23]. En él, la Audiencia Nacional (AN) eleva al TJUE una cuestión prejudicial (art. 267 del Tratado de Funcionamiento de la UE según el TL, en adelante TFUE) acerca de la delimitación del derecho fundamental de acceso y rectificación en lo que ha dado en llamarse «derecho al olvido» de los contenidos lesivos. En su resolución sobre esta cuestión prejudicial, el TJ ha afirmado una jurisprudencia avanzada y garante de la privacidad frente a la responsabilidad de los «motores de búsqueda» (Google) ante las eventuales lesiones de los derechos consignados en los arts. 7 y 8 CDFUE. Ya con posterioridad, el mismo TS (Sala de lo Civil, STS 4132/2015, de 15 de octubre de 2015) aplica la doctrina establecida en la cuestión prejudicial sobre el caso *Google Spain,* delimitando parámetros de ponderación de derechos en presencia: de un lado, los que corresponden a las denominadas «hemerotecas digitales» (de acuerdo con el derecho a «comunicar libremente información veraz» reconocido en el art. 20.1. d) CE); de otro, los que corresponden a los sujetos titulares de los datos almacenados en ellos. De acuerdo con el criterio clásico de la «veracidad» de los datos como canon dirimente del nivel de protección de las libertades informativas y de la comunicación (art. 20.1 CE), el TS ha establecido que las «hemerotecas digitales» no tienen «obligación» de cancelar ni bloquear el acceso a informaciones «veraces» en sus buscadores internos aun cuando correspondan a hechos o datos del pasado. Diferentemente, la doctrina jurisprudencial de la responsabilidad por los datos de las «indexaciones» que afecten al honor («reputación») del titular de los datos conlleva como consecuencia que esas hemerotecas digitales sí tengan la obligación de impedir su localización del titular de los datos por «motores de búsqueda» externos. Con lo que, dicho de otro modo, las hemerotecas son, sí, legalmente responsables de la «anonimización» externa… aunque no de la posibilidad de la «indexación» interna[24].

Este cuerpo jurisprudencial ilustra la comprensión de los pronunciamientos del TJUE que me propongo comentar más específicamente en las páginas que siguen: primeramente, la sentencia 8 de abril de 2014 en el llamado *Asunto Digital Rights Ireland*[25] (que afecta a la invalidación de la «Directiva de Retención de Datos» adoptada en 2006[26]); seguidamente, el llamado *Asunto Schrems*[27]

23 Asunto C-131/12, *Google Spain SL. y Google Inc. c. Agencia de protección de Datos (AEPD),* resuelto por sentencia del Tribunal de Justicia de 13 de mayo de 2014.

24 Véase, al respecto, Rodríguez-Izquierdo Serrano, M.: «Pluralidad de jurisdicciones y tutela de derechos: los efectos de la integración europea sobre la relación entre el juez ordinario y el Tribunal Constitucional», *Revista Española de Derecho Constitucional*, 2016, n.º 107, Madrid, 2016, pp. 117-150.

25 Sentencia del TJUE, de 8 de abril de 2014, asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland y Seitlinger y otros.*

26 Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, de «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».

27 Sentencia del TJUE, de 6 de octubre de 2015, relativa al asunto C-362/14, *Maximillian Schrems/ Data Protection Commissioner.*

(que afecta a la invalidación del Acuerdo *Safe Harbour*[28] adoptado en 2000 y, consiguientemente, a la interpretación del art. 20 de la Directiva de Protección de Datos 95/46 que consintió a la Comisión establecer, por el llamado procedimiento de comitología, una «decisión de adecuación» (*Adequacy Decision*) del «nivel de protección» dispensado a los derechos fundamentales de los ciudadanos europeos por un país tercero (en este caso, EEUU) con el que la UE había negociado y concluido aquel Acuerdo (el así denominado «Acuerdo de Puerto Seguro») para encuadrar el tráfico comercial de datos personales en las relaciones económicas, mercantiles y societarias de la relación transatlántica entre la UE y los EEUU[29].

Las consecuencias prácticas de una y otra sentencia del TJ han sido muy relevantes. La primera, *Asunto Digital Irelands*, ha conllevado la negociación y conclusión del llamado «*Umbrella Agreement*»[30] como cobertura y refuerzo de la protección de datos personales de los europeos en su transmisión a efectos de investigación de los delitos y lucha contra el crimen por las *Law Enforcement Agencies*, acuerdo que, en cuanto convenido en tratado internacional sujeto a la regla establecida en el art. 218 TFUE, sólo entra en vigor si el Parlamento «consiente» con su voto favorable. La segunda, el *caso Schrems*, ha conducido a la sustitución del llamado Acuerdo *Safe Harbour* por un nuevo *Privacy Shield*[31] («Escudo de Privacidad») revestido con mayores garantías para los datos personales y la transferencia de datos en las relaciones transatlánticas. Acompañando esta última sentencia, la Administración Obama comprometió en su día (septiembre de 2016) la aprobación por el Congreso de EEUU de un acceso a los recursos jurisdiccionales del sistema judicial de EEUU a los ciudadanos europeos que vean violados sus derechos sobre sus datos personales (la «*Judicial Redress Act*»[32], por la que se abre la vía de los *judicial remedies* a ciudadanos no estadounidenses).

28 Decisión 2000/520/CE, de la Comisión Europea, 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.

29 Cfr. el documentado studio publicado por el *Policy Department* del Parlamento Europeo *Transatlantic Digital Economy and Data Protection: State-of-Play and Future Implications for the EU's External Policies*, PE (Asuntos Exteriores), 2016.

30 Decisión (UE) 2016/2220 del Consejo de 2 de diciembre de 2016 relativa a la celebración, en nombre de la Unión Europea, del Acuerdo entre los Estados Unidos de América y la Unión Europea sobre la protección de los datos personales en relación con la prevención, la investigación, la detección y el enjuiciamiento de infracciones penales. El acuerdo entra en vigor el 1 de febrero de 2017.

31 Decisión de ejecución 2016/4176 de la Comisión de 12 de julio de 2016 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE.UU.

32 H.R.1428 — Ley de Recurso Judicial de 2015 promulgada por el presidente Obama el 24 de febrero de 2016, por la que se autoriza al Departamento de Justicia de EE. UU. a designar a otros países o a organizaciones regionales de integración económica cuyos ciudadanos podrán iniciar acciones civiles en virtud de la Ley sobre protección de la privacidad de 1974 contra determinados organismos gubernamentales estadounidenses con miras a acceder a los datos en posesión de dichos organismos, o a modificarlos, o a reparar la

Es obvio, ello no obstante, que la operatividad de tales avances penden a partir de ahora de la recién inaugurada Administración Trump (desde el 20 de enero de 2017), sin que ninguna señal emitida desde su elección por el actual presidente de los EEUU invite a ningún optimismo acerca de la calidad de la relación transatlántica escrutada desde el prisma del compromiso de respeto a la aproximación europea a la garantía de derechos y principios constitucionales[33].

II. LA PROTECCIÓN DE DATOS PERSONALES EN LA RELACIÓN TRANSATLÁNTICA. EL «ESCUDO DE PRIVACIDAD» UE-EEUU (*EU-US PRIVACY SHIELD*). LA PROTECCIÓN DE DATOS EN EL LLAMADO *UMBRELLA AGREEMENT* UE-EEUU

De modo que, efectivamente, resulta tan obligada una explicación somera —de otro modo, se haría en sí inabarcable— de la configuración y relieve del derecho fundamental a la protección de datos personales, a la privacidad, a la vida privada (intimidad) personal y familiar, como ámbito de protección reconocido a todas las personas en territorio de la UE de conformidad con la CDFUE y el TL, y como cuestión crucial, espinosa y a menudo divisoria, en la denominada «relación transatlántica» entre la UE y los EEUU.

Sólo a partir de ahí nos será posible una correcta comprensión de la secuencia normativa que conduce a la adopción del así llamado «Escudo de Privacidad» *(EU-US Privacy Shield*), determinado éste a su vez por el fallo de invalidez de la Directiva de Retención de Datos de 2006 en la sentencia del TJ de 8 de abril de 2014 (*caso Digital Rights Ireland*). Y por lo mismo procede, también, una breve aproximación a la Decisión *«Safe Harbour»*, objeto a su vez de enjuiciamiento y fallo de invalidez en la sentencia del TJ de 6 de octubre de 2016 (*Caso Schrems*), en el marco estructurado del diálogo y cooperación transatlántico de la UE con los EEUU.

La premisa asumida del cuadro de situación es fácil de formular: la UE y los EEUU muestran muy distintos enfoques y (por consiguiente) niveles de protección de los datos personales. Esta heterogeneidad afecta a la intensidad y calidad de las transacciones electrónicas de contenido económico y comercial (*e-commerce*), pero también, por extensión, a la relación transatlántica en toda su longitud y extensión.

En efecto, el último tramo descrito por el régimen jurídico convencional de los acuerdos que enmarcan la Decisión «*Safe Harbou*r» arranca en 2000. El *US Department of Commerce* reabrió entonces la negociación con la UE a la luz de las

divulgación ilícita de los registros transferidos desde un país extranjero a los Estados Unidos con el fin de evitar, investigar, detectar o perseguir delitos penales.

33 Vid. Weiss, M. A. y Archick, K.: «U.S.-EU Data Privacy: From Safe Harbour to Privacy Shield», *Congressional Research Service*, Washington D.C., 2016.

críticas relacionadas con la asimetría del nivel de protección de los datos personales en el conjunto de las relaciones económicas-comerciales transatlánticas. A la luz de la hoja de ruta descrita para la definitiva entrada en vigor de la CDFUE «con el mismo valor jurídico de los Tratados» junto al TL (art. 6 TUE), los derechos fundamentales han pasado a adquirir en la jurisprudencia del TJ un papel determinante del canon de validez del Derecho derivado, así como de adecuación de las legislaciones nacionales al Derecho europeo. Este es el contexto en el que cabe entender no sólo esta jurisprudencia sino las Resoluciones del PE y votos de «consentimiento» (o, en sentido contrario, rechazo) a la entrada en vigor de acuerdos con los EEUU, como fue el caso del llamado Acuerdo *«Swift»* entre la UE y EEUU[34] (TFTP, por sus siglas en inglés: *Terrorism Financiation Tracking Program*) rechazado en 2009 (y luego renegociado, conforme a las exigencias del PE), y más recientemente en el caso de la negociación del nonato *Transatlantic Trade and Investment Partnership* (TTIP), así como otros instrumentos y marcos de cooperación en los que se destaca la protección de datos.

Es cabalmente por ello que, en el régimen jurídico de la así llamada «decisión de adecuación» *(adequacy decision)* por la que la Comisión estima «adecuado» el nivel de garantía a los derechos de la privacidad conferido a los europeos por el ordenamiento de un país tercero, adquiere especial importancia la lectura del art. 25 de la Directiva de Protección de Datos 95/45 (posteriormente desplazada por el Reglamento adoptado en votación definitiva por el PE en abril de 2016[35], en el marco del llamado «*Data Protection Package*» junto a la Directiva orientada a proteger estos derechos en la lucha contra el crimen de las *Law Enforcement Agencies*[36]), así como la redefinición de la cooperación entre las autoridades europeas de protección de datos (*European Data Protection Supervisor* y *Data Protection Authorities* de los EE.MM) con las estructuras, organismos e instituciones previstas en los EEUU para cumplir funciones de supervisión y control de actores públicos y privados en el cumplimiento de estándares legales de privacidad[37].

34 Decisión del Consejo 2010/412/UE, de 13 de julio de 2010, relativa a la celebración del Acuerdo entre la Unión Europea y los Estados Unidos de América relativo al tratamiento y la transferencia de datos de mensajería financiera de la Unión Europea a los Estados Unidos a efectos del Programa de Seguimiento de la Financiación del Terrorismo, DO L 195, de 27 de julio de 2010.

35 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

36 Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo.

37 El *Data Protection Package* fue aprobado definitivamente por el PE el 14 de abril de 2016 (*Diario Oficial de la UE* de 4 de mayo de 2016) y disponiendo la Directiva de un plazo de transposición por los EE.MM hasta el 6 de agosto de 2018.

Sobre la base de su manifestación expresa de voluntad al respecto, las empresas y sociedades mercantiles norteamericanas pueden ahora adscribirse al llamado «Programa de Escudo de Privacidad» (*Privacy Shield*). Conforme a su régimen jurídico, pueden reabrir la transferencia de datos personales provenientes de la UE en caso de satisfacer las exigencias del dispositivo previsto, en todo caso más restrictivas que las habitualmente operativas en el tráfico mercantil doméstico estadounidense en el interior de EEUU. De acuerdo también con las nuevas pautas, la Comisión Europea y las Autoridades de EEUU deberán llevar a cabo «revisiones anuales» para la comprobación del funcionamiento del Programa, procediendo a repasar los eventuales incumplimientos que, en su caso, podrían acarrear la eventual suspensión o derogación de «decisiones de adecuación» por defecto de correspondencia con el denominado «nivel de protección adecuado y equitativo».

Para los intereses de la UE, el esquema así descrito comporta alguna ventaja respecto del precedente: confiere cierta unidad sistemática para la gestión y evolución de la multiplicidad de contactos y relaciones bilaterales, así como un título habilitante para la implicación práctica de las autoridades de protección de datos (Autoridad europea, el SEPD[38], y de los EE.MM, los DPAs[39]). De hecho, el ahora acordado «Escudo de Privacidad» contempla la supervisión continua de las autoridades de EEUU (*Department of Commerce* y *Federal Trade Commission*), así como una serie de disposiciones adicionales orientadas a asegurar que los ciudadanos europeos puedan interponer acciones de recurso administrativo y judicial. Entre otros, los siguientes:

a) Interposición de un recurso (corporativo, ante la propia empresa) que debe ser sustanciado y resuelto en plazo de 45 días;
b) derecho de acceso gratuito al denominado «mecanismo de resolución alternativa de disputas» (*ADR,* por sus siglas, en inglés);
c) derecho a la interposición de queja ante la autoridad nacional de protección de datos (*Data Protection Authority, DPAs,* por sus siglas en inglés*);*
d) derecho de acceso a un recurso ante un mecanismo específico y gratuito (asegurando el derecho de traducción del documento y de testificar por videoconferencia) y de resolución de disputas (*Privacy Shield Panel*) con carácter vinculante para las empresas que participen del «Escudo»;
e) derecho de acceso a la institución de un *Ombudsperson* de nueva creación con la estructura de la Seguridad Nacional de EEUU (Departamento de Estado);
f) acceso al recurso judicial incorporado en la llamada «*Judicial Redress Act*» impulsado en 2016 por la Administración Obama ante el Congreso de EEUU.

38 Supervisor Europeo de Protección de Datos (SEPD).

39 *Data Protection Authorities* (http://ec.europa.eu/justice/data-protection/article-29/structure/data-protection-authorities/index_en.htm).

Pese a los avances reconocibles respecto a la situación anterior, subsisten, sin embargo algunas objeciones serias. Tal y como se refleja en los debates sustanciados tanto en la Comisión de Libertades, Justicia e Interior del PE (Comisión LIBE) como en el Pleno de Estrasburgo, los principales puntos de preocupación y crítica expresados por los Grupos y miembros de la Eurocámara se resumirían como sigue:

a) Persisten, como no podría ser de otro modo, importantes diferencias a la hora de determinar las reglas aplicables para la protección de datos europeos en el Derecho de la UE respecto del estipulado por el »*Privacy Shield*» para las empresas y actores económicos que acepten voluntariamente someterse a sus obligaciones; por su parte, tampoco la jurisprudencia del sistema judicial de los EEUU arroja criterios tan sólidos y taxativos como los que se desprenden de la doctrina del TJUE;
b) Las prácticas de «vigilancia y supervisión masiva» (*mass surveillance*) que han venido estableciéndose en los EEUU (acceso de los Servicios de Inteligencia a los datos personales) no encuentran ni admiten parangón con la cultura jurídica, política y social imperante en el Derecho Europeo, tanto en el que dimana de fuentes jurídico-comunitarias como en el que caracteriza a los Derechos nacionales de los EE.MM. Se pone aquí de manifiesto un muy diferente nivel de asimilación del impacto de la «crisis de seguridad» activada alrededor del «terrorismo global», la «amenaza yihadista» y el crimen organizado en la sociedad estadounidense respecto de la respuesta, al menos hasta la fecha, de la ciudadanía europea y de sus instituciones: el «balance» o equilibrio tenso entre los vectores de libertad/seguridad se ha escorado en EEUU hacia la «securitización» con mucho mayor intensidad de cuanto puede observarse hasta ahora en la respuesta político-legislativa de escala paneuropea y, con los obligados matices y reservas, en los EE.MM de la UE;
c) De acuerdo con el Dictamen emitido por el llamado «*Working Party 29*» (Grupo de Trabajo de los DPAs de los EE.MM y el SEPD de la UE establecido en el art. 29 de la Directiva 95/46) cabe reconocer, sí, los «significativos avances» («*major improvements*») del actual *Privacy Shield* respecto del anterior *Safe Harbour*. Ahora bien, pervive la necesidad de clarificar cada caso de «decisión de adecuación» al objeto de especificar en modo entendible y nítido los mecanismos de «*redress*» (queja, rectificación) puestos a disposición del ciudadano/a acerca del tratamiento de sus datos personales en el marco del «Escudo».

De modo que cabe aceptar que el actual esquema no sólo sucede sino que mejora al anterior desde la perspectiva del «nivel de protección» que pueda estimarse «adecuado», al tiempo que se refuerza el dispositivo de garantía de su aplicabilidad y ejecución vinculante (*enforcement)*. En cuanto a los mecanismos de rectificación, se ensanchan y multiplican las posibilidades de recurso individual.

Y se preserva el objetivo de contribuir, asegurándolo, al tráfico mercantil y a la actividad económica de las empresas como un vector principal de la relación transatlántica entre la UE y EEUU.

Resta subrayar que, como hemos de ver, nada de lo aquí referido, aun en reseña acotada y con carácter sumario, habría tenido lugar ni hubiera sido entendible sin la aportación decisiva de la doctrina establecida por el TJUE en su función como garante del Derecho de la UE incluyendo, de manera resuelta y determinante, los derechos y principios dispuestos por la CDFUE como canon y parámetro de validez en sus enjuiciamientos del Derecho derivado y de los actos de la UE («decisión de adecuación» adoptada por la Comisión).

Así ha sido el caso de la sentencia *Digital Rights Ireland* sobre el esquema hasta entonces previsto por la Directiva de Conservación de Datos, tal como examinaremos en el apartado siguiente, determinando la adopción del ahora llamado «*Umbrella Agreement*» para el intercambio de datos personales que puedan mostrarse relevantes para la investigación de delitos graves transnacionales, la lucha contra el terrorismo y el crimen organizado. Pero también ha sido análogo el impacto de la sentencia *Schrems* sobre el Acuerdo *Safe Harbour*, sustituido ahora por el *Privacy Shield*[40].

Merece la pena completar la comprensión de este impacto con una somera referencia al *EU-US Umbrella Agreement*, acuerdo internacional negociado y acordado por la UE con los EEUU para garantizar la protección de datos en el marco de la cooperación judicial penal contra los delitos más graves[41].

El así llamado *Umbrella Agreement* se cualifica jurídicamente como un Acuerdo internacional (una forma de obligarse en Derecho internacional general, contemplada en el Convenio de Viena de Derecho de Tratados de 1969) entre la UE y los EE.UU. En cuanto tal, estipula obligaciones y derechos vinculantes para sus Partes en materia de protección de datos personales en supuestos de transferencia de los mismos en actos de cooperación en la investigación y persecución de los delitos (*Law enforcement cooperation*). Dicha transferencia de datos puede tener lugar tanto en aplicación de la legislación nacional de los EE.MM como sobre la base de Acuerdos internacionales concluidos por los EE.MM o por la propia UE con los EEUU.

La primera observación indica que el *Umbrella Agreement* no constituye en sí base jurídica autónoma (*legal basis*) para la autorización de transferencia de datos personales; su objeto es proporcionar garantías adicionales a otros Acuerdos de transferencia de datos ya anteriormente existentes, desde la premisa asumida de

40 Sobre la secuencia aquí resumida, vid: «How safe is the Safe Harbor? U.S and E.U Data Privacy Law and the enforcement of the FTC'S Safe Harbor program», *Boston University International Law Journal*, vol. 22 (2), pp. 399-424.

41 El 2 de diciembre de 2016, el Consejo adoptó la Decisión de Autorización de conclusión definitiva del Acuerdo; el 5 de diciembre, la UE y los EEUU completaron los procedimientos de aprobación definitiva en Declaración Conjunta. El acuerdo fue publicado en el *Diario Oficial de la UE* el 10 de diciembre de 2016.

la insuficiencia y límites del nivel de protección anteriormente imperante. Es, conviene saberlo, el primero de esta clase —Acuerdo internacional de protección de datos en áreas de cooperación policial y judicial penal contra la delincuencia— suscrito por la UE con los EEUU.

En efecto, el supuesto de hecho comprende que tanto la UE como sus EE.MM intercambian gran variedad y cantidad de datos personales con los EE.UU en el curso de investigaciones y procedimientos judiciales en la lucha contra el terrorismo y la delincuencia grave. Los instrumentos jurídicos hasta el momento existentes (Tratados de Asistencia Jurídica Mutua, entre otros) han venido siendo negociados muy mayoritariamente por los EE.MM, aun cuando exista ya algún ejemplo de Acuerdo negociado y concluido por la UE revestido de «personalidad jurídica única» en Derecho internacional (art. 47 TUE), tal y como es el caso problemático y notorio de los Acuerdos PNR (*Passengers Name Record*, «Registro de pasajeros», por sus siglas en inglés) con los EEUU[42], Canadá y Australia.

Conforme al *Umbrella Agreement*, los EEUU contraen la obligación de asegurar salvaguardias de protección de datos de ciudadanos europeos que respeten los principios del Derecho de la UE (incluyendo la lectura jurisprudencial del TJUE de la propia CDFUE, y el refuerzo que de sus derechos a la vida privada y a la protección de datos efectúa el aún reciente *Data Protection Package*, por el que un nuevo Reglamento sustituye a la anterior Directiva 95/46, complementado con una nueva Directiva para la cooperación policial y judicial penal contra los delitos graves). El nuevo esquema refuerza los derechos de los ciudadanos, delimitando los actos de recepción de datos por las autoridades estadounidenses: así, *purpose limitation*, control de veracidad (*accuracy*), transparencia, obligación de notificación de violaciones de la confidencialidad (*data breach*), garantías reforzadas para los datos sensibles, límites temporales a la conservación de los datos (*retention period*); refuerzo del consentimiento en las transferencias derivadas o secundarias (hacia terceros países) de los datos personales. Y, lo más importante, por vez primera establece el derecho de acceso a la rectificación y a los recursos judiciales de los ciudadanos europeos ante las autoridades y tribunales de EE.UU.

Tan crucial requerimiento fue abordado en la adopción por la *Judicial Redress Act* por el Congreso de EEUU por la Administración Obama (2016). Mediante esta disposición se supera por primera vez el déficit al respecto de la *US Privacy Act* de 1974 en EEUU, cuya garantía judicial protege a los ciudadanos estadounidenses exclusiva y excluyentemente. Por primera vez se sitúa en similar pie de igualdad (*equal footing*) el derecho de los ciudadanos estadounidenses a recurrir ante el sistema jurisdiccional europeo y el derecho de los europeos a acudir ante los tribunales de EEUU cuando defiendan su derecho de acceso a sus datos

42 Decisión del Consejo de 26 de abril de 2012 relativa a la celebración del Acuerdo entre los Estados Unidos de América y la Unión Europea sobre la utilización y la transferencia de los registros de nombres de los pasajeros al Departamento de Seguridad del Territorio Nacional de los Estados Unidos.

personales, rectificación o revelación ilícita (*unlawful disclosure*) y lesiva de su privacidad. En otros casos, los ciudadanos europeos dispondrán también de recursos administrativos y queja ante una autoridad de supervisión independiente en EEUU. En su conjunto, pues, y particularmente en este aspecto, el Acuerdo robustece las garantías disponibles en la panoplia ya existente de tratados bilaterales entre la UE o sus EE.MM con EEUU, muchos de los cuales habían sido lógicamente concluidos antes de la actualización y extensión del nivel de protección de datos operado por la aprobación definitiva, después de un *íter* prolongado e intensamente problemático (2009-2016), del *Data Protection Package* en 2016.

Haciendo esto, al mismo tiempo, el *Umbrella Agreement* incrementa la cooperación policial y judicial penal (*Law Enforcement Cooperation*). Refuerza el Derecho aplicable, la malla de Acuerdos y Tratados en el área instituida por el TL como «Espacio de libertad, seguridad y Justicia» (ELSJ, arts. 67 a 89 TFUE), y, consiguientemente, la seguridad jurídica en la transferencia de datos de la relación transatlántica[43]. De modo que si, en el futuro, hubieren de concluirse acuerdos bilaterales de transferencia de información, las garantías a cubierto de este Acuerdo Paraguas operarían sobre su objeto y los datos concernidos. El efecto esperable sería el de incentivar, facilitar y acelerar investigaciones conjuntas contra los delitos graves, el crimen transnacional, la delincuencia organizada y, por supuesto, el terrorismo. Intenta tener en cuenta que la transferencia de datos tiene lugar regularmente, sobre la base de las leyes nacionales actualmente vigentes o acuerdos internacionales cuyo nivel de garantía es inferior al dispuesto desde el *Umbrella Agreement*.

Pues bien, en este contexto importa también resaltar hasta qué punto este cuadro de referencias normativas y jurídico-internacionales se configura sometido de modo determinante al papel desempeñado por el TJUE a la vista de su función garante del «respeto del Derecho» (art. 19 TUE) y el carácter avanzado de su jurisprudencia. Así, en la actualidad, el Acuerdo PNR negociado y concluido por la UE y Canadá en la legislatura 2009-2014 (para sustituir al hasta entonces vigente desde 2005) pende de un pronunciamiento del TJ (recurso interpuesto, por cierto, por el PE). La doctrina que recaiga sobre este Tratado bilateral impactará con seguridad sobre otros Acuerdos PNR (caso del EU-US PNR). Sin embargo, es también cierto que el aquí comentado *Umbrella Agreement* reviste una naturaleza y función diferenciada de aquéllos, teniendo además un alcance y objeto de mayor envergadura. En efecto, el *Umbrella Agreement* no constituye en

43 Cfr. Martín y Pérez de Nanclares, J.: «El espacio de libertad, seguridad y justicia en el Tratado de Lisboa», *Revista de las Cortes Generales*, n.º 70-72, Madrid, 2007, pp. 85-126; y Jimeno Bulnes, M., «Las implicaciones del Tratado de Lisboa en la cooperación judicial europea en materia penal», en Arangüena Fanego, C., *Espacio Europeo de Libertad, Seguridad y Justicia*: *últimos avances en cooperación judicial penal*, Lex Nova, 201, pp. 48 a 70. Véase también mi propio análisis del Parlamento Europeo como legislador penal en López Aguilar, J.F: «El Parlamento Europeo, legislador del Espacio de Justicia Penal de la UE», *Revista de Derecho Político,* n.º 93, UNED, 2015.

sí base jurídica (*legal basis*) para transferencias de datos, revistiéndolas en cambio de mayores garantías y estándares de protección. Su listado de derechos y cláusulas de salvaguardia se cierne sobre los datos cuya transferencia autorizan preexistentes instrumentos (los ya referidos Tratados bilaterales), reforzando, eso sí, los derechos subjetivos de acceso, cancelación y recurso judicial. Especialmente novedoso, insisto, es este último punto, en la medida en que innova y recubre los estándares establecidos hasta entonces por los tratados PNR: nueva vía judicial que complementa lo dispuesto (con sus limitaciones en lo que respecta a EEUU) por las leyes nacionales. En su comparación con los Acuerdos PNR, las garantías del *Umbrella* recubren lagunas y fortalecen derechos accionables por los ciudadanos titulares de los datos, incluso (y singularmente) ante los supuestos conocidos como de «transferencia masiva» (*bulk data*) como es a menudo el caso de los PNR en cuanto a las obligaciones impuestas sobre compañías aéreas (*Air Carriers*).

Finalmente, persisten, como sucedía en el caso del *Privacy Shield* comentado, preocupaciones fundadas acerca de las insuficiencias y defectos del Acuerdo, expuesto por ello a la crítica como evidencian sus debates en el PE. Expuestas de manera sucinta, se concentran en dos puntos:

a) Ni el *Umbrella Agreement* ni la Judicial *Redress Act* contemplan la cobertura del derecho de acceso a la tutela judicial de ciudadanos no europeos en defensa de sus datos, pese a que la redacción de los arts. 7 y 8 de la CDFUE configuran su titularidad subjetiva con la mayor extensión reconociendo esos derechos a todas las personas, ciudadanos europeos (por serlo de un Estado miembro) o de cualquier país tercero. Es cierto, se alega al respecto, que la Judicial *Redress Act* beneficia solamente a ciudadanos europeos ante el sistema judicial de los EEUU, pero también que subsisten otras vías de protección administrativa estipuladas tanto en el *Umbrella Agreement* (derechos de acceso y de rectificación, recursos administrativos y quejas ante instituciones tipo *Ombudsman*) cuanto en el propio Derecho federal de los EEUU (*US Administrative Procedure Act*, *Freedom of Information Act*, *Electronic Communications Act*…). También es verdad, complementariamente, que el propio PE mandató a la Comisión la negociación de un Acuerdo con los EEUU, en su Resolución de 12 de marzo de 2014[44], adoptada tras las escandalosas revelaciones de la *mass surveillance* operada por la NSA de EEUU, que exigiera «*equal footing*» (pie de igualdad) en los derechos de los ciudadanos europeos respecto de los derechos de los estadounidadenses «*to provide effective and enforceable judicial remedies for all EU citizens in the UE without any discrimination*».

44 Resolución del Parlamento Europeo, de 12 de marzo de 2014, sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EE.UU., los órganos de vigilancia en diversos Estados miembros y su impacto en los derechos fundamentales de los ciudadanos de la UE y en la cooperación transatlántica en materia de justicia y asuntos de interior.

b) Se opone también que, en realidad, el *Umbrella* proporciona un «efecto equivalente» a una «*adequacy finding decision*», tal y como se criticó en la sentencia *Schrems*. En sentido contrario, los defensores de las ventajas del Acuerdo insisten en que no prejuzgan ni califican ni bendicen el «nivel de adecuación» del Derecho de EEUU en cuanto a protección de datos, limitándose, eso sí, a asegurar garantías adicionales y mayores a los datos y derechos afectados respecto del preexistente cuadro bilateral de instrumentos disponibles, que incluye Acuerdos vigentes (UE y EE.MM) y legislaciones nacionales[45].

En síntesis y en definitiva, el *Umbrella* provee un nivel suplementario de protección de datos en un área tan sensible como la que describe el ELSJ (arts. 67 a 89 TFUE) en la cooperación transatlántica para la investigación y enjuiciamiento de delitos graves transnacionales y terrorismo. Además, incorpora por vez primera el beneficio de acceso de ciudadanos europeos al sistema judicial de los EE.UU en defensa de sus datos y su privacidad (*Judicial Redress Act*). Para valorar su impacto, ha de tenerse en cuenta que los ciudadanos estadounidenses ya disfrutan actualmente de todas las reglas y estándares de protección de sus datos vigentes en Derecho europeo: incluido el importante salto adelante efectuado por el nuevo Reglamento de Protección de Datos y el *Data Protection Package*, que comprende significativas obligaciones para las empresas, el establecimiento de «delegados de empresa» y «encargados» de los datos, refuerzo del derecho de acceso a las autoridades nacionales de protección DPAs y, llamativamente, el establecimiento del llamado «derecho al olvido» que refuerza los de rectificación y/o cancelación de los contenidos lesivos[46].

Pues bien, por primera vez el *Umbrella* proporciona un nivel de protección razonablemente equivalente a los ciudadanos europeos ante la transferencia de sus datos a EEUU.

Por último, pese a las insoslayables y significativas distancias y diferencias existentes entre los respectivos estándares de protección y recursos disponibles en EEUU y en la UE —a ambas orillas del Océano en la relación transatlántica—, las ventajas observables en la ordenación ahora dispuesta respecto de la anterior son asimismo innegables. No se pierda de vista que, conforme al TL que refuerza

45 Acerca de los detalles de la secuencia aquí descrita, cfr. Moerel, L.: «An assessment of the impact of the Schrems judgement on the data transfer grounds available under EU data protection law for data transfers to the U.S.», Morrison Foerster LLP, 2016.

46 El *Data Protection Package* (nuevo Reglamento y Directiva) fue adoptado definitivamente por el Consejo el 8 de abril de 2016; y el 14 de abril de 2016 por el Parlamento Europeo. Publicado en el *Diario Oficial* de la UE el 4 de mayo de 2016, el Reglamento entró en vigor el 24 de mayo (plena efectividad el 25 de mayo de 2018). La Directiva está vigente desde el 5 de mayo de 2016, finalizando el plazo de transposición en los EE.MM el 6 de mayo de 2018. Sobre el derecho al olvido, véase la monografía de Rallo Lombarte, A.: *El derecho al olvido en Internet. Google v. Spain*, Centro de Estudios Políticos y Constitucionales, Madrid, 2014.

como nunca antes en su historia los poderes efectivos del PE como único órgano de la arquitectura europea legitimado directamente por el sufragio de la ciudadanía, ha sido el mismo PE el que ha dictado su última palabra al respecto, abriendo el cauce final para su entrada en su voto de «*consent*» (consentimiento y autorización del Tratado, art. 218 TFUE) en su Pleno de Estrasburgo de julio de 2016 (habiéndose previsto la fecha de 1 de febrero de 2017 para su efectiva vigencia y vinculatoriedad)[47].

III. DOS RELEVANTES SENTENCIAS DEL TJ CON IMPACTO EN LA RELACIÓN TRANSATLÁNTICA: LA SENTENCIA DEL TJ DE 8 DE ABRIL DE 2014 (*CASO DIGITAL RIGHTS IRELAND*) Y LA SENTENCIA DEL TJ DE 6 DE OCTUBRE DE 2015 (*CASO SCHREMS*): LOS DERECHOS DE LA CARTA DE DERECHOS FUNDAMENTALES DE LA UE COMO PARÁMETRO DE VALIDEZ DEL DERECHO EUROPEO

A partir de lo hasta aquí expuesto, solamente en el contexto que se acaba de describir cabe entender el llamado «Escudo de Privacidad» (*EU-US Privacy Shield*) como un reconocimiento del impacto vinculante de una línea jurisprudencial afirmada por el TJUE en garantía de los derechos de la CDFUE, parámetro de validez de todo el Derecho de la UE, incluyendo en su función garante del «respeto del Derecho» (art. 19 TUE) los Acuerdos internacionales y por ende los tratados por los que se articula la relación transatlántica con los EEUU.

Tal como hemos explicado en el apartado anterior, el Escudo de Privacidad viene a configurarse como un conjunto de reglas y normas de procedimiento cuya efectividad se confía a las autoridades estadounidenses con la finalidad de establecer un marco de protección equivalente al que rige en el Derecho europeo para todas las personas que se encuentren en territorio de la UE. Como instrumento para ese fin, la Comisión elabora una «decisión de adecuación» (*adequacy decision*) en procedimiento de comitología, de acuerdo con las previsiones del art. 25 de la anterior Directiva de Protección de Datos de 1995 (previa a la adopción definitiva, ya en 2016, del nuevo *Data Protection Package*, con un notable refuerzo del consentimiento como garantía de los titulares de los datos y de sus derechos de acceso, rectificación y cancelación, incorporando un (acotado) «derecho al olvido» (*right to be forgotten*) para la eliminación de contenidos lesivos para la reputación o imagen del ciudadano lesionado en sus derechos, e introduciendo obligaciones para las empresas e instituciones).

47 El 28 de noviembre de 2016, el Pleno de Estrasburgo votó, además, su Recomendación (Ponente: J.P. Albrecht) sobre los Proyectos de Decisión del Consejo sobre el «Acuerdo entre EEUU y la UE para la protección de información personal en la prevención, investigación, detención y enjuiciamiento de los delitos» (el llamado *Umbrella Agreement*).

El objeto de esta decisión reside en la verificación por parte de la Comisión acerca de la protección de los datos personales transferidos desde la UE hacia los EEUU (empresas estadounidenses que participan del «escudo»). Sólo en caso afirmativo (la protección de esas empresas se estima «adecuada» a los estándares del Derecho europeo), se autorizará la transferencia a los efectos del tráfico transatlántico (relaciones mercantiles, económicas y comerciales).

Toca ahora explicar las dos sentencias elegidas para ilustrar el impacto de la jurisprudencia del TJUE basada en la interpretación del alcance vinculante de los derechos de la CDFUE, y de manera singular en los reconocidos en sus arts. 7 y 8: derecho a la privacidad y derecho a la protección de los datos personales.

1. *Digital Rights Ireland* y la Directiva europea de Conservación de Datos

En primer término, en su sentencia *Digital Rights Ireland* (8 de abril de 2014) el TJ hace valer su interpretación del alcance de los derechos establecidos en los arts. 7 y 8 en conexión con lo dispuesto en sus arts. 51 a 54 CDFUE (especialmente, en el art. 52) para delimitar, en su regulación bajo reserva de ley que en todo caso respete su «contenido esencial», el alcance de los principios constitucionales de necesidad y de proporcionalidad subordinada a un fin legítimo.

Concretamente, en los Asuntos Acumulados C-293/12 y 594/129, sentencia del TJ de 8 de abril de 2014, el TJ (Gran Sala) resuelve declarar inválida la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, de «conservación de datos (*Data Retention*) 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». El TJ declara esta invalidez desde la entrada en vigor de la Directiva (efecto *ex tunc*).

Ha de tenerse presente que el objetivo declarado de la Directiva de Conservación de Datos era el de armonizar las disparidades legales en los ordenamientos de los EE.MM sobre consecución de datos generados o tratados por servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones, garantizando la disponibilidad de esos datos con el fin de preservación, investigación, detención y enjuiciamiento de delitos graves, como delincuencia organizada y terrorismo. La Directiva establecía el deber de conservación de los datos de tráfico y localización, y la necesaria para identificar al abonado o al usuario; no así, importa subrayarlo, el contenido de la comunicación ni la información consultada.

Tanto la *High Court* de Irlanda como el *Verfassungsgerichtshof* de Austria (TCF austríaco) habían requerido prejudicialmente al TJ el examen de validez de la Directiva de conservación de datos, tanto a la luz del TL como de la CDFUE (art. 7, 8 y 11: respeto a la vida privada y datos de carácter personal, en conjugación con el derecho a la libertad de expresión y de comunicación por cualquier

medio, incluidas las comunicaciones electrónicas.). Complementariamente, la cuestión interpuesta por el TCF de Austria solicita la anulación de la concreta Ley federal austríaca que transpuso la Directiva en el Derecho austríaco.

En su pronunciamiento, el TJ viene a señalar que los datos permiten saber ciertamente con qué persona y de qué modo concreto se produce en cada caso la comunicación, lugar y frecuencia durante un periodo de tiempo determinado o determinable. Y que, en su conjunto, estos datos pueden proporcionar información muy precisa sobre hábitos de vida cotidiana, lugares de permanencia o estancia, desplazamientos, actividad, relaciones sociales o medios frecuentados.

Al regular normativamente la obtención y tratamiento de estos datos, establece el TJ en su resolución que «la Directiva se inmiscuye e interfiere gravemente en la garantía de los derechos fundamentales de las personas». Y se trata, consiguientemente, de dilucidar si esa injerencia objetivamente grave se encuentra justificada por su subordinación a una finalidad legítima, y, en segundo lugar, si esta inmisión o injerencia responde o no al objetivo de «lucha por la seguridad y contra la delincuencia transnacional» de acuerdo con los principios de necesidad y de proporcionalidad de las medidas que impacten sobre los derechos de la CDFUE (art. 52).

Concluye en su razonamiento el TJ que al adoptar la Directiva de conservación de datos, el legislador de la UE ha sobrepasado los límites impuestos por los principios de necesidad y de proporcionalidad impuestos por la CDFUE (art. 52)

Haciendo esto, además, la sentencia incorpora los siguientes criterios interpretativos del alcance de los derechos de los arts. 7 y 8 como parámetros de validez del Derecho derivado:

a) la Directiva abarca de manera generalizada todas las personas, medios de comunicación electrónica y datos susceptibles de tráfico; no reconoce ni establece, pues, ninguna diferencia, limitación o excepción en función del objetivo proclamado por la norma que es, declaradamente, la seguridad y la lucha contra los delitos graves;
b) la norma europea enjuiciada no fija ningún criterio de delimitación de propósito (*purpose limitation clause*): el acceso a los datos personales —sensibles, «íntimos» o no— sólo puede disponerse en el marco de la Directiva para el objetivo lícito de prevenir, detectar o reprimir delitos graves;
c) no consta que exista tampoco ninguna delimitación espacial del territorio europeo: la Directiva no obliga a que el delito sea cometido o consumado en territorio de la UE;
d) Finalmente, el período de conservación de los datos (mínimo de 6 meses, máximo de 24) no guarda tampoco ninguna conexión explícita con la utilidad específica de los datos para la consecución del objetivo proclamado: no se constata tampoco en lo relativo a la «*retention period clause*» ninguna delimitación de los principios constitucionales de necesidad («lo estrictamente necesario») y de proporcionalidad consagrados en la CDFUE (art. 52 CE).

2. *Schrems*, Acuerdo *Safe Harbour* y Directiva de Protección de Datos

En la segunda sentencia reseñada en estas líneas, el llamado *Asunto Schrems* (sentencia del TJ de 15 de octubre de 2015), el TJ resuelve, en cambio, declarar la invalidez de un acto de Derecho derivado, con alcance interpretativo sobre la Directiva de Protección de Datos 95/46 (posteriormente sucedida por el nuevo Reglamento de Protección de Datos adoptado definitivamente en 2016, ya en la legislatura 2014-2019 del Parlamento Europeo, en el marco del llamado «*Data Protection Package*»: Reglamento y Directiva para la protección de datos en la lucha contra el crimen por las *Law Enforcement Agencies*). Ese acto de Derecho derivado es la Decisión de la Comisión de «Puerto Seguro» (*Safe Harbour*) y declara que EEUU «garantiza un nivel de protección adecuado a los datos personales transferidos». Pero en la práctica ha supuesto la renegociación de un Acuerdo que sustituye a éste —el *Privacy Shield* (2016)—, con lo que extiende a este ámbito de la relación transatlántica el impacto vinculante de la doctrina del TJUE sobre los derechos de la CDFUE.

En efecto, al declarar la invalidez de la Decisión, el TJ declara también que junto a la competencia exclusiva del TJ para declarar la invalidez del acto de las instituciones de la UE, las autoridades nacionales de control pueden examinar si la transferencia de datos de una persona a otro país respeta o no las exigencias de la legislación de la UE sobre protección de datos, así como acudir también a los tribunales nacionales, al igual que la propia persona interesada, a fin de plantear ante el TJ una cuestión prejudicial sobre la validez de la Decisión de que se trate.

Así, la Directiva 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 (Directiva 95/46 del Parlamento Europeo y del Consejo, de 24 de octubre de 1995) dispone que solo se puede transferir datos a un país tercero (EE.UU, por ejemplo) si «dispone de un nivel de protección adecuado». También la Comisión puede declarar («A*dequacy Decision*») si un país tercero garantiza o no «nivel de protección». La Directiva determina que cada EE.MM debe designar «autoridades nacionales de control».

El ciudadano austríaco Maximilian Schrems, un reconocido activista contra los abusos contra la privacidad perpetrados en la red, singularmente vigilante ante los llamados «gigantes» y que se proclama en su recurso «usuario de Facebook desde 2008», impugna ante la Justicia irlandesa que sus datos personales son trasferidos desde la filial irlandesa del servidor en territorio de EE.UU. A raíz de la resolución del notorio *Caso Snowden* (el escándalo de la *mass surveillance* sobre los datos personales de ciudadanos europeos por parte de la *National Security Agency*, NSA, de EEUU), Schrems plantea una acción judicial concretamente dirigida contra la actividad de servicios de información de la *NSA* de EEUU. La Autoridad nacional irlandesa de protección de datos (DPA) desestimó la reclamación elevada a este respecto, puesto que en la Decisión de 26 de julio de 2000

adoptada por la Comisión (Decisión 2000/520/CE[48]) se afirma la» adecuación» del Derecho de EEUU en el marco del llamado «régimen» (en realidad, un Acuerdo bilateral de EEUU con la UE) de «Puerto Seguro» (*Safe Harbour*) para fijar la garantía de un nivel adecuado de protección de datos personales en la relación transatlántica.

El TJ procede a valorar la consistencia del «test de seguridad nacional», impuesto por los EEUU de acuerdo con su «interés público en la prevención de amenazas y delitos» potencialmente indeterminados, para concluir que los estándares y procedimientos impuestos por los EEUU prevalecen sobre las garantías y filtros del régimen de «Puerto Seguro». Dicho con otras palabras, constata que las *Authorities* de EEUU ignoran («dejan de emplear») las reglas de protección de los datos transferidos cuando entran «en conflicto con la seguridad».

En consecuencia, el TJ establece que el Derecho de la UE no ha acertado a «limitarse a lo estrictamente necesario» cuando autoriza sin control ni garantía suficiente la transferencia a EEUU de los datos personales de cualesquiera ciudadanos (sean europeos, o no) desde territorio europeo *(i.e,* los EE.MM). Lo que conduce a la decisión de reparar, estimando la demanda, la consiguiente lesión sobre el contenido esencial de los derechos fundamentales a la vida privada y a la protección de los datos, tal y como los consagran los arts. 7 y 8 CDFUE, parámetro de validez del ordenamiento europeo.

Complementariamente, el TJ critica en la referida sentencia que las normas enjuiciadas no prevean tan siquiera la posibilidad de que pueda ser utilizada ninguna acción jurisdiccional de rectificación, cancelación o supresión de los datos objeto de conservación, lo que vulnera el contenido esencial del derecho fundamental de acceso a la Justicia y tutela judicial efectiva consignado en el art. 47 de la CDFUE.

Finalmente, el TJ declara que la Decisión de 2000 «priva» ilegítimamente a las autoridades de control de sus propias facultades para la verificación de los casos en que cualquier persona resuelva impugnar el alcance o términos de una decisión de «adecuación» en garantía de la regla del «respeto a la vida privada» (art. 7 CDFUE). Restringe así la Decisión impugnada las competencias legítimas de las autoridades nacionales de control.

Así, en definitiva, el TJ dictamina que la Decisión es inválida y no ofrece ni asegura ninguna «protección adecuada» a los datos personales. La consecuencia es inapelable: debe, con efectos *ex tunc*, a partir de la sentencia *Schrems*, cesar toda transferencia de datos hacia EEUU, haciéndose urgente negociar un nuevo marco jurídico para esta concreta dimensión de la relación transatlántica (los anteriormente explicados acuerdos *Privacy Shield* y el llamado *Umbrella Agreement*).

48 2000/520/CE: Decisión de la Comisión, 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.

IV. CONCLUSIONES

Como hemos expuesto sumariamente, el 8 de abril de 2014, el Tribunal de Justicia (Gran Sala), institución de la UE a la que los Tratados distinguen como máximo intérprete y garante de la validez y eficacia del ordenamiento jurídico comunitario (art. 19 TUE), dictó una relevante sentencia con impacto decisivo en la relación transatlántica en el Asunto conocido como *Digital Rights Ireland*. Resolvía en ella varios asuntos acumulados (C-293/12 y C-594-12) en cuestiones prejudiciales planteadas (art. 267 TFUE) por la *High Court* Irlandesa y el *Verfassungsgerichtshof* (TC) austríaco. En su fallo, el TJ declara inválida la Directiva 2006/24 CE, de «conservación de datos» (*Data Retention Directive*), sentando doctrina jurisprudencial sobre los derechos de la privacidad consagrados en los arts. 7, 8 y 11 de la CDFUE que entró en vigor con el TL, en conexión con aspectos cruciales de la regulación de las transmisiones electrónicas de datos personales y los servicios de acceso a redes públicas de comunicación.

El 6 de octubre de 2015, el mismo TJ (Gran Sala) resuelve otra relevante cuestión prejudicial planteada por la *High Court* de Irlanda en el llamado *caso Schrems* (*Maximilian Schrems v. Data Protection Commissioner*), también ésta revestida de impacto determinante en la relación transatlántica. En su fallo, el TJ declara inválida la Decisión 2000/520 de la Comisión, por la que, con arreglo a una lectura inaceptable del art. 25 de la Directiva 95/46 de Protección de Datos, constata que EE.UU «garantiza un nivel de protección adecuado» a los derechos de la privacidad de los ciudadanos europeos (*Adequacy Decision*), confiriendo a este tercer país el estatus de «puerto seguro» (*Safe Harbour*).

Estos dos pronunciamientos del TJ completan su ya amplia y consistente doctrina jurisprudencial en materia de derechos fundamentales al tiempo que efectúan de consuno un paso adelante de gran significación en la protección de los derechos de la privacidad —derecho a la intimidad personal y familiar (art. 18 CE), derecho a la «vida privada» (art. 8 CDFUE)— ante la revolución tecnológica e informacional de las comunicaciones electrónicas y la digitalización del tratamiento automatizado de los datos personales.

Es por esta relevante dimensión que he seleccionado estas dos sentencias del TJ para comentar, en síntesis sumaria, los muy interesantes problemas suscitados en el Derecho europeo a propósito de las cuestiones señaladas: derecho a la privacidad y sociedad en red, contrastando los parámetros y estándares de protección en ambas orillas del Atlántico.

La contribución del TJUE al *Decision Making Process* de la UE forma parte de una historia con capítulos extensos; pero continúa activa, singularmente en el ámbito que mejor puede, a mi juicio, a restaurar el vínculo de ese proceso decisional —inevitablemente revestido de notable sofisticación y complejidad que alimenta la percepción de «distancia»— con la ciudadanía europea. Reforzar la protección de sus derechos proclamados es un objetivo plausible, y es éste un vector principal de la actividad del TJ.

Lo he afirmado y sostenido en anteriores escritos: hace tiempo que, en una UE ensombrecida por el pésimo manejo de la peor crisis de su historia —la que arrancó con la «Gran Recesión» de 2008 y se ha cronificado como «glaciación» del espíritu de la integración supranacional, últimamente arrollado por la regresión nacionalista y el auge de los populismos—, las únicas buenas noticias a las que hemos asistido durante estos largos años han provenido a pares del PE (el *Data Protection Package* sería un ejemplo en este campo) y del TJ.

En las páginas precedentes me he propuesto extractar, siquiera apretadamente, la secuencia histórica de la normativa y decisiones europeas enjuiciadas por el TJ, así como un comentario acerca de sus consecuencias. Y ello por una razón clara. Porque, entre otras cosas, prueban hasta qué punto encuadrar adecuadamente el régimen jurídico de la «retención de datos» y la «*decisión de Safe Harbour*» resulta crucial para entender los procesos negociadores de las soluciones jurídicas objeto de discusión en el marco de la relación bilateral transatlántica entre la UE y EEUU: El nuevo «*Privacy Shield*» (Escudo de Privacidad) que debe dar cobertura a la transmisión de datos en las relaciones económicas, comerciales y financieras entre empresas y actores económicos del tráfico mercantil entre EEUU y la UE; y el llamado «*Umbrella Agreement*», que debe dar cobertura a toda transmisión transatlántica de datos que se estimen relevantes en la lucha contra el crimen (cooperación de las *Law Enforcement Agencies* en materia de investigación de los delitos transnacionales e identificación, detención, persecución y enjuiciamiento de los presuntos responsables).

En ambos planos, la doctrina jurisprudencial del TJ ha resultado y resulta en todo determinante. Pero también el papel desempeñado por el PE. No sólo porque, una vez más, nos ha brindado una ocasión de subrayar el impresionante refuerzo del perfil institucional y del papel legislador del Europarlamento (colegislador, junto al Consejo) en materias de gran relieve constitucional como el *Espacio de Libertad, Seguridad y Justicia* (ELSJ, Título V, arts. 67 a 89 TFUE), singularmente el emergente Derecho penal europeo, o el desarrollo normativo de los derechos fundamentales consagrados en la CDFUE (respetando en todo caso su «contenido esencial», art. 52), siendo como es el PE el único órgano de la UE directamente legitimado por el sufragio universal de los 500 millones de ciudadanos europeos. No sólo por ello, insisto, sino también y sobre todo porque la reorientación de la relación transatlántica con los EEUU pasa necesariamente por el derecho del PE a pronunciar la última palabra al respecto del procedimiento completo de negociación y acuerdo, con carácter vinculante, en su definitivo voto de «*consent*» («consentimiento»), o no, en los acuerdos internacionales negociados y concluidos por la UE (art. 218 TFUE)[49].

49 Sobre este, relativo al robustecimiento del Parlamento Europeo como institución motriz de la legitimación directamente electiva del proceso decisional europeo y como colegislador junto con el Consejo en

Y es asimismo claro que en la reorientación de la relación transatlántica —la estratégica cooperación de la UE con los EEUU—, el PE ha tenido en cuenta la jurisprudencia del TJ en una materia tan sensible y querida para la representación electiva de la ciudadanía como es la que concierne al nivel de protección que gocen los ciudadanos europeos ante las empresas y autoridades estadounidenses.

Así ha sido el caso, en modo muy particular, en todo lo relativo al acceso equitativo a recursos administrativos y jurisdiccionales (*access to remedies and Judicial Redress*) ante eventuales lesiones de su privacidad en la masiva transmisión electrónica de datos personales que ha experimentado el impacto de la revolución tecnológica e informacional, en un momento de la historia en que la seguridad —la «securitización»— ha emergido como nunca como prioridad política —en consecuencia al flagelo del crimen organizado, el terrorismo global y la «radicalización» de la amenaza yihadista—, con una fuerza de choque sobre nuestros ordenamientos (y sobre el frágil equilibrio «libertad/seguridad») inédita hasta el tiempo presente.

***

TITLE: *The Habeas Data in the Last CJEU Doctrine.*

ABSTRACT: *Right from the first very chapters of the European construction under the Treaty of Rome (1957), which turns 60 this year 2017, the jurisprudence by the Court of Justice has truly been decisive to shape the constitutional dimension of the European Community legal order. In a series of historical decisions, the CJEU has affirmed its primacy, its binding efficacy and unity, while guaranteeing its uniform interpretation and implementation. But it has also, above all, enshrined the fundamental rights resulting from the common constitutional traditions as a source of European Law (i.e general principles). This legal doctrine has been ultimately consolidated in positive Law, finally, with the entry into force of the Treaty of Lisbon (TL) in 2009, incorporating the TEU, the TFEU and, most notably, the Charter of Fundamental Rights of the EU (CFREU) with the «same legal value as the Treaties». Charter Fundamental Rights have turned to be, consequently, a parameter for examining the validity of secondary EU legislation, as well as for scrutinizing and reviewing the standard of compatibility of the national legislation of EU Member States with European law.*

The legal doctrine of the ECJ on fundamental rights has been particularly relevant in its impact on the data protection in the framework of the rights to privacy, privacy with regard to the electronic data transfer, and access to judicial protection of these rights (art. 7, 8 and 47 CFREU). It combines the principles of reservation of law (in due respect of its essential content) as well as proportionality and necessity for legislative measures that might affect them. But, moreover, this doctrine has had a decisive impact on the legal articulation of the so-called transatlantic partnership between the EU and the US, confronting data protection standards on both sides of the Atlantic and imposing guarantees of an «adequate level of protection» for all European citizens.

This paper explores the impact of two recent relevant decisions by the ECJ — its rulings on Digital Rights Ireland case (2014) and on the Schrems case (2015) — upon the secondary EU legislation (Data Retention Directive of 2006, Data Protection Directive of 1995, and the «adequacy» Decision of the

ámbitos antes reservados a los EE.MM o a la cooperación intergubernamental, me remito a lo que he expuesto en LÓPEZ AGUILAR, J.F: *La UE: suicidio o rescate. Del mito del rapto a Europa a la tentación de la autodestrucción*. Editorial Tirant Humanidades, Madrid, 2013.

European Commission of 2000), as well as upon International Law instruments (Safe Harbour Agreement) between the EU and the US. It imposes, as a consequence, not only a negotiation that remedies the shortcomings detected in both decisions, but also a compelling updating of European law itself (new Data Protection Package in 2016) and a new US federal law, which, for the first time ever, provides European citizens with access to judicial remedies in U.S. Courts in defending their right to data protection (Judicial Redress Act, 2016).

Resumen: *Desde los primeros capítulos de la construcción europea con el Tratado de Roma (1957) que cumple 60 años, la jurisprudencia dictada por el Tribunal de Justicia ha sido determinante para la dimensión constitucional del ordenamiento comunitario. En una secuencia de decisiones históricas, el TJ ha afirmado su primacía, eficacia vinculante y su unidad garantizando su interpretación y aplicación uniforme, pero también, sobre todo, los derechos fundamentales dimanantes de las tradiciones constitucionales comunes como fuente del Derecho europeo (principios generales). Esta doctrina se consolida en Derecho positivo, al fin, con la entrada en vigor del Tratado de Lisboa (TL) en 2009, incorporando el TUE, el TFUE, y, relevantemente, la Carta de Derechos Fundamentales de la UE (CDFUE) con el «mismo valor jurídico que los Tratados» y, consiguientemente, parámetro de validez de todo el Derecho derivado, así como de enjuiciamiento de la compatibilidad de la legislación de los EE.MM con el Derecho europeo.La doctrina del TJUE sobre derechos fundamentales ha sido su proyección sobre la protección de datos en el marco de los derechos a la vida privada, a la privacidad frente a la transferencia electrónica de datos y al acceso a la tutela judicial de estos derechos (art. 7, 8 y 47 CDFUE). En ella conjuga los principios de reserva de ley (respetando su contenido esencial) y de proporcionalidad y necesidad de las medidas que les afecten. Pero, además, esta doctrina ha adquirido un impacto decisivo en la articulación jurídica de la relación transatlántica entre la UE y EEUU, confrontando los estándares de protección de datos a ambos lados del Atlántico e imponiendo garantías de un «nivel de protección adecuado» para los ciudadanos europeos.*

Este artículo examina el impacto de dos recientes sentencias relevantes del TJ —Asunto Digital Rights Ireland (2014) y Asunto Schrems (2015)— sobre el Derecho derivado (Directiva de Conservación de Datos de 2006, Directiva de Protección de Datos de 1995, y Decisión de «adecuación» de la Comisión Europea de 2000) y sobre instrumentos de Derecho internacional (Acuerdo Safe Harbour) entre la UE y EEUU. Impone, como consecuencia, no sólo una negociación que repare las deficiencias detectadas en ambas resoluciones sino una actualización del Derecho europeo (nuevo Data Protection Package en 2016) y una novedosa Ley federal de EEUU que por primera vez ofrece a los ciudadanos europeos acceso al sistema de recursos judiciales ante los tribunales estadounidenses en la defensa del derecho a la protección de datos (Judicial Redress Act, 2016).

Key words: *Fundamental Rights.*

Palabras clave: *Derechos fundamentales, Carta de Derechos de la UE, vida privada, privacidad y protección de datos, doctrina jurisprudencial del TJUE, Directivas europeas de Conservación de Datos y de Protección de Datos, Data Protection Package, relación transatlántica UE-EEUU, Acuerdos UE-EEUU, Escudo de Privacidad (Privacy Shield) y Umbrella Agreement.*

Fecha de recepción: *23.12.2016* Fecha de aceptación: *01.02.2017*