W

WORKING
PAPERS

350

El régimen jurídico de las transferencias internacionales de datos personales. Especial mención al marco regulatorio *Privacy Shield*

ALBERT CASTELLANOS RODRÍGUEZ

ICPS
Institut de Ciències Polítiques i Socials
Adscrit a la Universitat Autònoma de Barcelona

El régimen jurídico de las transferencias internacionales de datos personales. Especial mención al marco regulatorio *Privacy Shield*

ALBERT CASTELLANOS RODRÍGUEZ

Abogado especializado en derecho tecnológico

WP núm. 350

Institut de Ciències Polítiques i Socials

Barcelona, 2017

El Institut de Ciències Polítiques i Socials (ICPS) es un consorcio creado en 1988 por la Diputación de Barcelona y la Universitat Autònoma de Barcelona, institución esta última a la que está adscrito a efectos académicos.

"Working Papers" es una de las colecciones que edita el ICPS, previo informe del correspondiente Comité de Lectura, especializada en la publicación –en la lengua original del autor– de trabajos en elaboración de investigadores sociales, con el objetivo de facilitar su discusión científica.

Su inclusión en esta colección no limita su posterior publicación por el autor, que mantiene la integridad de sus derechos.

Edición: Institut de Ciències Polítiques i Socials (ICPS)
Mallorca, 244, pral. 08008 Barcelona (España)
http://www.icps.cat

ISSN: 1133-8962
DL: B-10186-2012

1. ENFOQUE DE LAS TRANSFERENCIAS INTERNACIONALES DE DATOS DE CARÁCTER PERSONAL BAJO EL ACERVO DEL REGLAMENTO (UE) 2016/679 GENERAL DE PROTECCIÓN DE DATOS. MENCIÓN AL ANTEPROYECTO DE LEY ORGÁNICA EN ESPAÑA

En los últimos tiempos, como consecuencia del rápido avance de la sociedad tecnológica y la globalización, hemos sido espectadores de los cambios que han supuesto estos factores en la manera de relacionarse de los ciudadanos, barajándose circunstancias que hasta el momento no habían sido tenidas en cuenta, como el aumento de los movimientos transfronterizos de datos de carácter personal, dado su valor fundamental en la actual sociedad de la información.

A la luz de los cambios digitales aludidos, las transferencias internacionales de datos personales han ido adoptando una posición primordial en los textos normativos que se han ido sucediendo paulatinamente sobre la materia. Cabe citar, a título de ejemplo, la ya derogada Ley Orgánica 5/1992, conocida comúnmente bajo el acrónimo LORTAD[1], que ya abordaba estas cuestiones con cierta polémica por el amplio espectro de dudas que esta disciplina arrojaba, tanto para los propios órganos legislativos como para el sector doctrinal y los propios sujetos obligados a su cumplimiento.

En el contexto descrito no existía, hasta la entrada en vigor del Reglamento (UE) 2016/679[2] General de Protección de Datos (en adelante, RGPD o Reglamento) –que aborda este asunto con mayor simpatía–, una definición sobre las transferencias internacionales de datos personales legislativamente adoptada en el ámbito español. Debemos remontarnos a inicios de siglo para encontrar la primera referencia sobre este concepto. En concreto, se citaba en la norma primera de la Instrucción 1/2000[3], de 1 de diciembre, de la Agencia Española de Protección de Datos (en adelante, AEPD), cuando, al señalar su ámbito de aplicación, preceptuaba que: "La presente Instrucción será de aplicación a cualquier supuesto de transferencia internacional de datos de carácter personal. A tal efecto, se considera transferencia internacional de datos toda transmisión de los mismos fuera del territorio español. En particular, se consideran como tales las que constituyan una cesión o comunicación de datos y las que tengan por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero […]".

A este respecto, cabe señalar que la referida Instrucción fue objeto de anulación parcial a través de dos sentencias que entraron a valorar su contenido. Inicialmente podemos citar la sen-

[1] Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. En línea: https://www.boe.es/buscar/doc.php?id=BOE-A-1992-24189 [consultado el 15.08.2017].

[2] 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). En línea: https://www.boe.es/doue/2016/119/L00001-00088.pdf [consultado el 15.08.2017].

[3] Instrucción 1/2000, de 1 de diciembre, de la Agencia de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos. En línea: https://www.boe.es/buscar/doc.php?id=BOE-A-2000-22726 [consultado el 15.08.2017].

tencia de la Audiencia Nacional, de 15 de marzo de 2002[4], y posteriormente la sentencia del Tribunal Supremo, de 25 de septiembre de 2006[5].

Por todo ello, usualmente se relacionaba de manera errónea el concepto analizado a aquellas transmisiones o comunicaciones de datos que se realizaban fuera del territorio español, máxime si tenemos en cuenta el redactado del artículo 34, letra k) de la Ley Orgánica 15/1999[6] (en adelante, LOPD). No obstante, es preciso apuntar que las transferencias internacionales de datos tienen tal consideración cuando las mismas se producen fuera del Espacio Económico Europeo[7], como más adelante se tendrá ocasión de comprobar.

Efectuado este apunte, y a los efectos de intentar delimitar el concepto objeto de análisis, se hace preciso seguir con lo suscitado en España al respecto, donde encontramos, en primera instancia, que el artículo 3, en su letra c) de la LOPD, ya preceptúa a las transferencias internacionales de datos personales como una de las operaciones de tratamiento, pero no es en segunda instancia, hasta la entrada en vigor del Reglamento 1720/2007[8] (en adelante, RLOPD), donde encontramos una definición expresa sobre este concepto, en concreto, lo hacemos en su artículo 5, apartado primero, letra s), cuando dispone que: "Transferencia internacional de datos: tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo, bien constituya una cesión o comunicación de datos, bien tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero establecido en territorio español".

Desde la perspectiva del derecho comunitario, el concepto fue inicialmente introducido por la Directiva 95/46/CE[9], dado que la misma tenía como objetivo primordial tratar de armonizar las normativas internas de los distintos Estados miembros en materia de protección de datos de carácter personal para que los movimientos transfronterizos de datos en el seno de la Unión Europea no

[4] Sentencia de la Sala de lo contencioso-administrativo de la Audiencia Nacional, de 15 de marzo de 2002, Sección Primera. Fundamento jurídico decimotercero. En línea: https://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/audiencia_nacional/common/pdfs/Sentencia_AN_15_3_2002_y_Sentencia_TS_Recurso_Casacion_25_9_2006.pdf [consultado el 15.08.2017].

[5] Sentencia de la Sala de lo contencioso-administrativo del Tribunal Supremo, de 25 de septiembre de 2006, Sección Sexta (Recurso de Casación núm. 3223/2002). Fundamento jurídico quinto. En línea: https://www.agpd.es/portalwebAGPD/canaldocumentacion/sentencias/audiencia_nacional/common/pdfs/Sentencia_AN_15_3_2002_y_Sentencia_TS_Recurso_Casacion_25_9_2006.pdf [consultado el 15.08.2017].

[6] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. En línea: https://www.boe.es/buscar/pdf/1999/BOE-A-1999-23750-consolidado.pdf [consultado el 15.08.2017].

[7] A este respecto, es preciso mencionar que la Ley Orgánica 15/1999 únicamente hace mención de los Estados miembros ubicados en el seno de la Unión Europea, sin incluir a Islandia, Liechtenstein y Noruega, dado que los mismos forman parte del denominado Espacio Económico Europeo. Sin embargo, a tenor de diversas resoluciones e informes emitidos por la AEPD, cabe afirmar que los movimientos de datos personales destinados a los países anteriormente mencionados no serán entendidos como transferencias internacionales de datos personales en el sentido estricto del término.

[8] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. En línea: https://www.boe.es/buscar/act.php?id=BOE-A-2008-979 [consultado el 15.08.2017].

[9] 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. En línea: http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:31995L0046 [consultado el 15.08.2017].

encontrasen ningún tipo de salvedades, al mismo tiempo que se intentaba articular un procedimiento de tutela y protección sobre los derechos reconocidos a los residentes en territorio europeo.

Con posterioridad, y como respuesta a las dificultades que supuso que los distintos Estados miembros adoptasen una regulación similar sobre la protección de los datos personales de sus respectivos ciudadanos, las autoridades europeas que disponen de competencias sobre la materia han decidido variar el instrumento jurídico para conseguir el efecto armonizador, optando por la aplicación del anteriormente referenciado Reglamento General de Protección de Datos, dado que, con su eficacia directa[10], se pretende poner fin a la diversidad de normativas existentes en el marco de la Unión Europea.

Una vez sentado lo anterior, dentro del marco de las transferencias internacionales de datos personales, cabe aducir dos figuras relevantes que participan en el conjunto de este proceso, destacándose al respecto que su conceptualización aparece recogida en la Decisión de la Comisión, de 5 de febrero de 2010[11], a través de su artículo 3, donde se establece, por un lado, que el exportador de datos será "el responsable del tratamiento que transfiera los datos personales" y, por otro lado, al importador de datos lo define como "el encargado del tratamiento establecido en un tercer país que convenga en recibir del exportador datos personales para su posterior tratamiento en nombre de este, de conformidad con sus instrucciones y los términos de la presente decisión, y que no esté sujeto al sistema de un tercer país que garantice la protección adecuada en el sentido del artículo 25, apartado 1, de la Directiva 95/46/CE".

En consonancia con la exposición contenida en el párrafo anterior, y haciendo un ejercicio de analogía con las vicisitudes jurídicas que se contienen en el RGPD, podemos advertir que estas figuras se encuentran también amparadas bajo el acervo del susodicho cuerpo legal. De una parte, al responsable del tratamiento se le define como "la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros"[12].

De otra parte, podemos aducir la introducción de la figura del destinatario, que se asemejaría a la del importador de los datos personales en el marco de un movimiento transfronterizo de los mismos, la cual se expone como "la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho

[10] En relación con este punto, es importante traer a colación el artículo 291, apartado 1, del Tratado de Funcionamiento de la Unión Europea, cuando señala que "los Estados miembros adoptarán todas las medidas de Derecho interno necesarias para la ejecución de los actos jurídicamente vinculantes de la Unión". Cuando se requieran condiciones uniformes de ejecución de los actos jurídicamente vinculantes de la Unión, la Comisión ejercerá competencias de ejecución (artículo 291, apartado 2, del TFUE).

[11] Decisión de la Comisión, de 5 de febrero de 2010, relativa a las cláusulas contractuales tipo para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo [notificada con el número C (2010) 593]. En línea: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32010D0087 [consultado el 15.08.2017].

[12] Artículo 4, apartado 7.º, del Reglamento General de Protección de Datos.

de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros"[13].

Una vez tenemos debidamente identificados a los actores principales que intervienen en las transferencias internacionales de datos personales, cabe entrar a diseccionar los novedosos cambios que la reciente regulación europea ha establecido para las mismas, puesto que el esquema que se sigue no difiere en demasía del que se preveía originariamente en la Directiva 95/46/CE, sino que se ha optado por reforzar algunos extremos que hasta el momento no ofrecían la seguridad jurídica que resulta aplicable a este tipo de actividades de tratamiento.

Así pues, en aras a propiciar mecanismos de cooperación internacional y salvaguarda para los derechos de los interesados, el RGPD parte, en primer lugar, de un principio general de prohibición, amparado en el Capítulo V del referido texto comunitario –que es el que regula íntegramente esta materia–, que encuentra su excepción únicamente cuando el país, territorio, sector u organismo internacional destinatario de los datos personales objeto de transferencia ofrezca un nivel de protección adecuado, se aporten las suficientes garantías que permitan la viabilidad de la operación o, en su defecto, el supuesto de hecho concreto se pueda enmarcar en alguna de las circunstancias establecidas como excepciones, de conformidad con el texto del reglamento.

En segundo lugar, se ha equiparado la posición jurídica del encargado a la del responsable del tratamiento, haciéndole extensibles las mismas obligaciones que hasta el momento únicamente eran aplicables a los responsables por lo que atañe al cumplimiento de la legislación vigente en materia de protección de datos de carácter personal. Ello viene propiciado por las dificultades que hasta el momento se venían sucediendo para efectuar la subcontratación de terceros para la prestación de determinados servicios en terceros países, intentando favorecer así tales cuestiones[14].

En tercer lugar, se ha ampliado el espectro de destinatarios de los datos personales en el marco de las transferencias internacionales, dado que en la anterior Directiva 95/46/CE el eje vertebrador se focalizaba sobre la figura del "tercer país", pero en la actual regulación vemos cómo se ha optado por introducir adicionalmente un nuevo concepto de "organización internacional", y que aparece inicialmente recogido como parte del texto incluido en el título del Capítulo V del RGPD –dedicado a regular esta materia–, convirtiéndose, por ende, en toda una declaración de intenciones.

En cuarto lugar, el planteamiento de las decisiones de adecuación cambia parcialmente de perspectiva, esto es, en la anterior regulación[15], se dejaba esencialmente en manos de los Estados

[13] Artículo 4, apartado 9.º, del Reglamento General de Protección de Datos.

[14] A tenor de lo comentado, cabe recordar que, a efectos del artículo 26, apartado 2, de la 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; y 33 y 70.2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter General (LOPD) y de su Reglamento de desarrollo, aprobado por el Real Decreto 1720/2007, de 21 de diciembre (RLOPD), respectivamente, la AEPD aprobó una serie de cláusulas contractuales para la transferencia de datos personales a los subencargados del tratamiento establecidos en terceros países que no garanticen una adecuada protección de los datos personales.

[15] Conviene subrayar, al respecto, la importancia de la Decisión 2008/615/JAI del Consejo, de 23 de junio de 2008, sobre la profundización de la cooperación transfronteriza, en particular en materia de lucha contra el terrorismo y la delin-

miembros esta decisión, tal y como se desprende del tenor literal introducido en la redacción del artículo 25, apartado primero, de la reiterada Directiva, cuando establece que: "Los Estados miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente pueda efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado".

No obstante, a lo anterior, el propio artículo aludido, en su apartado sexto, facultaba a la Comisión para que pudiera efectuar un reconocimiento similar al otorgado para los Estados miembros, pero en este caso con efectos en todo el territorio comunitario, no únicamente en el marco de la soberanía nacional que se le reconoce a cada Estado. Tal eficacia ha tenido el uso de esta competencia por parte de la Comisión que, en la actualidad, las autoridades de control europeas no han realizado pronunciamientos individuales en este sentido, sino que se trata de una facultad que, en la práctica, le ha quedado reservada en régimen de exclusividad al órgano europeo.

Como consecuencia del planteamiento aducido, el Reglamento parte de esta concepción como la posibilidad por antonomasia para que se pueda realizar el reconocimiento de una decisión de adecuación de un tercer país o una organización internacional como un destino que garantice un nivel de protección adecuado en materia de protección de datos de carácter personal.

Avanzando en nuestro razonamiento, resulta conveniente remarcar que los criterios que se seguían en la Directiva 95/46/CE para evaluar la adecuación del nivel de protección[16] no resultaban tan extensivos como los que se apuntan en el nuevo régimen previsto en el Reglamento General de Protección de Datos, destacándose especialmente cuando se refiere, entre otras cuestiones, a la valoración sobre "el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional observadas en ese país u organización internacional, la jurisprudencia, así como el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recur-

cuencia transfronteriza, así como la Decisión Marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, dado que intentar salvaguardar la ausencia de regulación que establece la Directiva 95/46/CE sobre este asunto, debido a la exclusión que se efectúa sobre aquellos datos que tengan como objetivo la seguridad pública y las actividades del Estado en el ámbito penal.

[16] En referencia a este punto, el artículo 25, apartado segundo, establecía lo siguiente: "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".

sos administrativos y acciones judiciales que sean efectivos […]"[17], dado que en jurisdicciones como la estadounidense, donde la legislación es ampliamente sectorial, respaldada con mecanismos de autorregulación, estas precisiones acotadas por el Reglamento adoptan una importancia trascendental a la hora de determinar la viabilidad de una decisión.

De ahí que, una vez valorados todos los elementos que preceptúa el artículo 45, apartado segundo, del RGPD, se faculta a la Comisión para que decida, mediante un acto de ejecución[18], si un tercer país u organización internacional goza de un nivel de protección adecuado, siendo por ende obligatorio que ese concreto acto de ejecución lleve aparejado un procedimiento de revisión de, al menos, cada cuatro años, que permita valorar periódicamente las circunstancias que llevaron a la consecución de tal decisión. En este mismo sentido, cabe destacar que el Reglamento sigue manteniendo la vigencia de aquellas autorizaciones emitidas por los Estados miembros y/o sus autoridades de control, así como de aquellas decisiones adoptadas por la Comisión[19] –en ejercicio de sus competencias–, en tanto en cuanto no resulten modificadas, sustituidas o derogadas.

En quinto lugar, conviene señalar los dos condicionantes cumulativos que han sido objeto de introducción en el Reglamento[20], esto es, en un primer término, la necesidad de ofrecer garantías adecuadas, y, en un segundo término, la imperiosa obligación de que los interesados dispongan de "derechos exigibles" y "acciones legales efectivas", traduciéndose ello en un intento de reforzar las garantías de las que disponen los afectados sobre el control de sus datos personales.

En relación con lo manifestado en el párrafo anterior, se ha procedido a la división de las garantías adecuadas en dos tipologías diferenciadas. Por un lado, aquellas donde no se precisa ninguna autorización expresa por parte de una autoridad de control nacional[21]. Aspecto, este último, que se ha tenido en cuenta para ampliar el catálogo de instrumentos que hasta el momento había disponibles, en detrimento de la anterior regulación –Directiva 95/46/CE–, tal y como suce-

[17] Artículo 45, apartado 2.º, letra a), del Reglamento General de Protección de Datos.

[18] Artículo 291 del Tratado de Funcionamiento de la Unión Europea. En línea: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:12012E291 [consultado el 15.08.2017].

[19] A este respecto, cabe mencionar aquellos países que en la actualidad gozan de un nivel de protección adecuado, los cuales se pueden ordenar de la siguiente manera: a) Suiza (Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000); b) Canadá (Decisión 2002/2/CE de la Comisión, de 20 de diciembre de 2001, respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos); c) Argentina (Decisión 2003/490/CE de la Comisión, de 30 de junio de 2003); d) Guernsey (Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003); e) Isla de Man (Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004); f) Jersey (Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008); g) Islas Feroe (Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010); h) Andorra (Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010); i) Israel (Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011); j) Uruguay (Decisión 2012/484/UE de la Comisión, de 21 de agosto de 2012); k) Nueva Zelanda (Decisión 2013/65/UE de la Comisión, de 19 de diciembre de 2012); l) Estados Unidos. Aplicable a las entidades certificadas en el marco del escudo de privacidad UE-EE.UU. Decisión (UE) 2016/1250 de la Comisión, de 12 de julio de 2016. AEPD. Transferencias internacionales de datos. Países con un nivel adecuado de protección. En línea: https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides-idphp.php [consultado el 15.08.2017].

[20] Artículo 46, apartado 1.º, del Reglamento General de Protección de Datos.

[21] Artículo 46, apartado 2.º, del Reglamento General de Protección de Datos.

de con los esquemas de certificación, los códigos de conducta y las normas corporativas vinculantes, comúnmente denominadas bajo el acrónimo BCR[22].

Con respecto al último de los instrumentos citados, es decir, las normas corporativas vinculantes, vemos cómo el Reglamento ha optado por su reconocimiento legal, por ser un mecanismo habitualmente utilizado por los grupos y/o conglomerados de empresas multinacionales que precisan, para la correcta llevanza de sus negocios y actuaciones jurídicas, un elevado número de operaciones transfronterizas con datos personales, hecho que favorece la adopción de este tipo de instrumentos. Dicho reconocimiento ha sido posible como consecuencia de un arduo trabajo[23] en los últimos años, llevado a término por el Grupo de Trabajo del Artículo 29[24] (en adelante, GT29), para que se posibilite la utilización de las BCR en aquellos Estados miembros donde su validez y utilización no estaba legalmente amparada.

Por otro lado, consideremos ahora aquellas garantías adecuadas que precisan una autorización de la autoridad de control nacional competente[25] para desplegar su efectividad, las cuales podrán ser aportadas mediante "cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional" o "disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados".

En definitiva, se trata de modificaciones que redundan en facilitar la cooperación internacional y las relaciones comerciales, pero que, a su vez, intentan salvaguardar los intereses y derechos que la legislación aplicable le reconoce a los afectados.

En sexto lugar, resulta preciso hacer alusión a uno de los últimos artículos que el Reglamento recoge sobre la materia objeto de análisis, esto es, los supuestos de excepción para situaciones específicas[26], que, en gran medida, resultan similares a los estipulados en la anterior regulación –Directiva 95/46/CE– y, especialmente, a lo recogido en el artículo 34 de la LOPD, y que facultan a los sujetos obligados para que, en determinados supuestos, puedan ejecutar transferencias internacionales de datos personales sin disponer de una decisión de adecuación o de las garantías adecuadas referenciadas con anterioridad.

[22] *Binding Corporate Rules*, por sus siglas en inglés.

[23] Resulta oportuno señalar el Documento WP 107, relativo al "Procedimiento de Cooperación para el Establecimiento de una Opinión Común sobre la Adecuación de las Medidas Adoptadas en las *Binding Corporate Rules*", que el Grupo de Trabajo del Artículo 29 adoptó el 14 de abril de 2005. En línea: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp107_en.pdf [consultado el 15.08.2017]. También diversos documentos de análisis y comentarios que se han sucedido posteriormente sobre esta cuestión.

[24] Podríamos definir al Grupo de Trabajo del Artículo 29 como un organismo de consulta independiente, creado bajo el amparo de la anterior Directiva 95/46/CE, que está formado por representantes de la totalidad de las autoridades de control nacionales de los Estados miembros, así como por el Supervisor Europeo de Protección de Datos y representantes también de la propia Comisión Europea, que se encarga principalmente del estudio y análisis relativos a la aplicabilidad de la legislación europea en materia de protección de datos de carácter personal. Para obtener más información sobre el presente órgano, se ruega consultar el siguiente enlace: http://www.agpd.es/portalwebAGPD/internacional/Europa/grupo_29_europeo/index-ides-idphp.php [consultado el 15.08.2017].

[25] Artículo 46, apartado 3.º, del Reglamento General de Protección de Datos.

[26] Artículo 49 del Reglamento General de Protección de Datos.

Sin embargo, se han introducido ciertas cuestiones que resultan interesantes de resaltar, como, en primera instancia, sucede con el hecho de que se disponga del consentimiento del interesado para efectuar la transferencia propuesta. En este punto, se ha introducido la necesidad de que el afectado haya "sido informado de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas". Ello deberá de realizarse siempre con carácter previo, recogiéndose así las reiteradas peticiones que venía efectuando al respecto, en los últimos tiempos, el GT29.

En segunda instancia, se ha habilitado una especie de "cajón de sastre" a través del último inciso del apartado primero del artículo 49, cuando se afirma: "Cuando una transferencia no pueda basarse en disposiciones de los artículos 45 o 46, incluidas las disposiciones sobre normas corporativas vinculantes, y no sea aplicable ninguna de las excepciones para situaciones específicas a que se refiere el párrafo primero del presente apartado, solo se podrá llevar a cabo si no es repetitiva, afecta solo a un número limitado de interesados, es necesaria a los fines de intereses legítimos imperiosos perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado, y el responsable del tratamiento evaluó todas las circunstancias concurrentes en la transferencia de datos y, basándose en esta evaluación, ofreció garantías apropiadas con respecto a la protección de datos personales. El responsable del tratamiento informará a la autoridad de control de la transferencia. Además de la información a que hacen referencia los artículos 13 y 14, el responsable del tratamiento informará al interesado de la transferencia y de los intereses legítimos imperiosos perseguidos", que contradice, *a priori*, las intenciones de protección que el texto del Reglamento viene manifestando a lo largo de la multitud de los considerandos iniciales.

Todo y que el redactado del texto está orientado hacia la acumulación de requisitos que deberían de dificultar su aplicabilidad, cierto es que será interesante esperar la interpretación que se efectúe por parte de las autoridades de control sobre cada uno de los condicionantes que se incluyen, dado que, en su inmensa mayoría, se trata de conceptos jurídicos indeterminados que pueden suponer el riesgo de inmiscuirse en interpretaciones distanciadas del principio de seguridad jurídica, tal y como podría ocurrir, a título de ejemplo, con la institución de los "intereses legítimos imperiosos", que en la práctica se ha acotado su utilización a supuestos concretos tasados.

En tercera y última instancia, se han realizado diversas matizaciones sobre el texto que ya incorporaba la anterior Directiva, y que han venido a clarificar las interpretaciones que se podían efectuar sobre el texto inicial fruto todo ello, de la experiencia que se ha ido obteniendo en los últimos tiempos, como consecuencia de la aplicación práctica de tales cuestiones.

Como último punto a comentar del presente apartado, debemos hacer mención obligatoriamente al nuevo Anteproyecto de Ley Orgánica de Protección de Datos[27], que en la actualidad se

[27] Para mayor información relacionada con esta cuestión, se ruega consultar el siguiente enlace: http://www.mjusticia.gob.es/cs/Satellite/Portal/1292428446044?blobheader=application%2Fpdf&blobheadername1=ContentDisposition&blobheadername2=Medios&blobheadervalue1=attachment%3B+filename%3D170623_Anteproyecto_LO_Protecci%C3%B3n_de_Datos.pdf&blobheadervalue2=1288795476854 [consultado el 15.08.2017].

encuentra en fase de tramitación, y que producirá la derogación de la actual Ley Orgánica 15/1999, así como del Reglamento 1720/2007, que la desarrolla.

Ante esta tesitura, el redactado del que se ha dotado al nuevo cuerpo legal realiza una adaptación de lo estipulado en el RGPD y hace mención a ciertas particularidades relacionadas con los mecanismos mediante los cuales las autoridades de control nacionales pueden realizar ciertas actividades y desplegar, por ende, el ejercicio de sus competencias. Todo ello se ha articulado mediante la introducción del Título V, dedicado a las transferencias internacionales de datos (artículos 41 a 44).

Resulta preciso adicionar, además, que mediante nota de prensa[28] publicada el pasado 26 de julio de 2017 por parte del Consejo General del Poder Judicial[29] (en adelante, CGPJ), se daba a conocer que el pleno del susodicho órgano había aprobado, con carácter unánime, el informe que ha elaborado en lo relativo a la transposición del RGPD al ordenamiento jurídico español, estableciendo al respecto que: "Se advierte en el anteproyecto una cierta falta de coherencia con la función y finalidad propia de una norma que ha de limitarse a adecuar y, en su caso –y con la configuración que ha hecho la jurisprudencia europea de esta función–, complementar el Reglamento europeo. En ocasiones, señala el informe, el articulado propuesto traspasa los límites de esas funciones, pues algunos artículos resultan innecesarios, otros reiterativos, y otros van más allá en sus marcos reguladores".

En este sentido, el referido comunicado indica que el eje central del informe del CGPJ se ha desarrollado en torno a la disposición adicional quinta del Anteproyecto, referente a la autorización judicial en materia de transferencias internacionales de datos, resaltándose la sugerencia efectuada sobre la introducción de mejoras técnicas en la redacción del mismo que resulten alineadas con las preceptuadas por el derecho alemán y, literalmente, se indica que el susodicho órgano consideraría más adecuado que la nueva legislación sobre la materia previese "la completa configuración de un procedimiento judicial desde el cual se va a entablar el diálogo prejudicial, a raíz de la solicitud de la decisión judicial formulada por la autoridad de control que conoce de la reclamación, y cuya resolución depende de la validez de la decisión de la Comisión".

[28] Si desea realizar su consulta, se ruega dirigirse al siguiente enlace: http://www.poderjudicial.es/cgpj/es/Poder-Judicial/Consejo-General-del-Poder-Judicial/Sala-de-Prensa/Notas-de-prensa/El-CGPJ-propone-articular-un-procedimiento-judicial-completo-para-resolver-las-reclamaciones-contra-las-transferencias-internacionales-de-datos-personales [consultado el 15.08.2017].

[29] El artículo 122, ap. segundo, de la Constitución Española de 1978, define al Consejo General del Poder Judicial como "órgano de gobierno del mismo". En línea: https://www.boe.es/legislacion/documentos/ConstitucionCASTELLANO.pdf [consultado el 15.08.2017].

2. EVOLUCIÓN DE LA DECISIÓN DE LA COMISIÓN, DE 26 DE JULIO DE 2000, SOBRE LOS PRINCIPIOS DE PUERTO SEGURO (*SAFE HARBOR*)

(i) Antecedentes

La Decisión de la Comisión, de 26 de julio de 2000[30], ya en sus iniciales considerandos, establece que, aunque exista un común acuerdo de voluntades para intentar articular mecanismos de cooperación y transparencia que permitan una mejora de las relaciones comerciales y transaccionales entre los Estados Unidos de América y la Unión Europea, hay que poner de manifiesto que se parten de sistemas regulatorios antagónicamente diferentes, que aunque intenten proteger el mismo bien jurídico, esto es, la privacidad (en el ámbito comunitario, se acuña bajo la denominación de protección de datos personales), lo realizan a través de mecanismos legales diferentes.

A grandes rasgos, podemos diferenciar que en los Estados Unidos de América se parte de un sistema que no reconoce la protección de la privacidad mediante una legislación específica, sino que ello se efectúa a través de normativas sectoriales[31] que, mediante la complementación de reglamentaciones y códigos de adhesión, propician un marco regulador singular que difiere del conceptuado en el ámbito europeo, tendente a vehicular toda la regulación sobre una misma materia a través de un único cuerpo legal.

En este mismo sentido, y a mayor abundamiento, se hace preciso destacar que ni la Constitución Federal de los Estados Unidos de América de 1787 ni sus correspondientes enmiendas reconocen expresamente un *right to privacy*, tal y como se ha mencionado con anterioridad, sino que el Tribunal Supremo, a lo largo de su vacilante jurisprudencia, lo ha considerado como una cuestión implícita en diversos lindes, tal y como ocurre: **(i)** dentro de la libertad de asociación garantizada por la Primera Enmienda; **(ii)** en la salvaguarda que introduce la Cuarta Enmienda ante registros arbitrarios (*unreasonable searches and seizures*); **(iii)** en la Quinta Enmienda, cuando se refiere a la protección frente a la incriminación de uno mismo y la obligación de revelar información de carácter personal; **(iv)** en la reserva de derechos que se incluye en la Novena Enmienda; y por último, **(v)** en el concepto de libertad sustantiva que el Tribunal Supremo ha interpretado respecto de la cláusula del debido proceso legal[32] (*due process of law*) de la Decimocuarta Enmienda,

[30] 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 [notificada con el número C (2000) 2441]. En línea: http://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:32000D0520 [consultado el 20.08.2017].

[31] Podemos citar, entre otras, a título de ejemplo, la *Right to Financial Privacy Act* (RFPA) de 1978; la *Financial Services Modernization Act* de 1999, habitualmente conocida como la *Gramm-Leach-Bliley Act (GLBA)*; la *Fair and Accurate Credit Transactions Act* (FACTA) de 2003; por lo que hace referencia a datos médicos, la *Health Insurance Portability and Accountability Act* (HIPAA) de 1996; y con mayor actualidad, en lo relativo a la privacidad genética, podríamos citar la *Genetic Information Nondiscrimination Act* (GINA) de 2008. Haciendo énfasis igualmente en la protección de la información personal en las comunicaciones electrónicas, cabe citar, en especial, la *Cable Communication Policy Act* (CCPA) de 1984; la *Electronic Communications Privacy Act* (ECPA) de 1986; la *Telecomunications Act* de 1996; la *Children's On-line Privacy Protection Act* (COPPA) de 1998; y la *E-Government Act* de 2002.

[32] Chicago, Burlington & Quincy Railroad Company v. City of Chicago, 166 U. S. 226 (1897).

que finalmente se traduce en la adopción del concepto de *Informational Privacy*, durante la década de los setenta, referido al poder del afectado de controlar el flujo de su información personal.

Por todo lo expuesto, y con el objetivo de articular un marco legislativo que hiciera efectivo el cumplimiento de los requisitos normativos que establecía la Directiva por parte de las organizaciones estadounidenses, el Departamento de Comercio de los Estados Unidos de América y la Comisión Europea destinaron más de dos años a amplias negociaciones para desarrollar el contenido de la Decisión, lo cual posibilitó que finalmente, el 26 de julio de 2000, se adoptara el texto, articulándose un mecanismo que habilitaba las transferencias de datos personales de ciudadanos europeos a empresas que tenían su sede en Estados Unidos, siempre que las mismas, con carácter previo, hubieran aceptado respetar los principios de salvaguarda y protección a la privacidad contenidos en el acuerdo de puerto seguro.

(ii) Contenido

El contenido y la estructura de la Decisión de la Comisión, de 26 de julio de 2000, se compone, en primer lugar, por once considerandos iniciales; en segundo lugar, por seis artículos que intentan plasmar el calado jurídico de la norma; en tercer lugar, el Anexo n.º1 formula los "Principios de puerto seguro (Protección de la vida privada)" y, en cuarto lugar, el Anexo n.º 2 se refiere a las preguntas más frecuentes (FAQ, por sus siglas en inglés)[33] para finalmente, en el último tramo de la norma, incorporar una serie de anexos, que llegan hasta el número sexto, y que tienen como principal objetivo intentar arrojar luz y facilitar la aplicabilidad práctica del texto de la Decisión y las correspondientes FAQ[34].

En este sentido, cabe subrayar que la decisión de adherirse a los principios consagrados en la Decisión gozaba de carácter voluntario para las organizaciones estadounidenses, a través de un mecanismo de autocertificación[35] que les permitía valorar individualmente si cumplían con los referidos principios y obligaciones que les resultaban de aplicación para que, posteriormente, pudieran comunicarlo al Departamento de Comercio de los Estados Unidos, dado que era el organismo regulador al que se le habían atribuido tales competencias.

Sin perjuicio de lo anterior, se pueden resumir brevemente los principios que se encuentran recogidos en el Acuerdo de Puerto Seguro –que se configuran como una opción de mínimos–, a través de la siguiente enumeración: **(i) principio de notificación**: se establece la obligación de informar a los afectados sobre las finalidades de utilización de sus datos personales; **(ii) principio de opción**:

[33] *Frequently Asked Questions*.

[34] Tal y como lo ha establecido al respecto el GT29, las preguntas más frecuentes y el propio texto de la Decisión deberán entenderse como formantes de un mismo cuerpo jurídico unitario y con carácter vinculante. Para su consulta, se aporta el enlace para conocer las opiniones que se han emitido al respecto por el susodicho Grupo: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1999/wp23_en.pdf [consultado el 20.08.2017].

[35] Se trataba de un procedimiento que gozaba de un amplio margen de discrecionalidad y que no aportaba la suficiente seguridad jurídica en referencia a la protección de los datos de carácter personal. Ello fue puesto de manifiesto también por el GT29, a través de la Opinión 7/1999, de fecha 3 de diciembre de 1999, que puede consultarse en: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1999/wp27_en.pdf [consultado el 20.08.2017].

hace referencia a la posibilidad de solicitar a los afectados su consentimiento para realizar comunicaciones de datos a terceros, así como utilizar sus datos para finalidades distintas para los que fueron inicialmente recabados; **(iii) principio de ulterior transferencia**: señala la necesidad de que, para que se pueda realizar una cesión de datos personales a terceros, la empresa destinataria deberá de estar adherida a los principios de puerto seguro, respetar las disposiciones establecidas en la Directiva 95/46/CE, así como efectuar un contrato que obligue a la adopción de las medidas de seguridad y protección que resulten aplicables; **(iv) principio de seguridad**: preceptúa que las organizaciones que se encargan de recabar datos de carácter personal apliquen todas las precauciones necesarias que permitan evitar su pérdida, uso indebido, acceso no autorizado, divulgación, alteración o destrucción.

Siguiendo con el análisis que se viene efectuando hasta el momento, cabe seguir enumerando lo siguiente: **(v) principio de integridad de los datos**: determina que las organizaciones únicamente pueden utilizar los datos personales de acuerdo con las finalidades para las que fueron recabados, es decir, deben de ser pertinentes para el uso previsto y la información debe ser precisa, completa y actualizada; **(vi) principio de acceso**: recoge el derecho de los interesados a tener acceso a los datos personales de los que dispongan las organizaciones sobre los mismos, así como a poder modificarlos, corregirlos o suprimirlos en caso de inexactitud.

Y, por último, **(vii) principio de cumplimiento**: establece la necesidad de que las organizaciones articulen mecanismos para que los interesados, en el supuesto de que no se respeten las vicisitudes contenidas en el Acuerdo de Puerto Seguro, puedan disponer de vías de recurso que les ofrezcan y faciliten una tutela de sus derechos y que, además, si resulta procedente, se deriven consecuencias en el supuesto de incumplimiento como, por ejemplo, la imposición de indemnizaciones. Sin embargo, cabe advertir que, en la práctica, el régimen sancionador previsto ha adolecido de una ausencia de efectividad, dado que su formulación era tan generalista y poco concreta que ha provocado, como resultado, su no aplicación de manera extensiva.

A este respecto, resulta necesario traer a colación que la propia Comisión Europea, en su informe emitido en fecha 20 de octubre de 2004[36], ya alertaba sobre el hecho de que gran multitud de organizaciones norteamericanas no se sujetaban al cumplimiento de lo establecido en los principios de puerto seguro para la protección de la privacidad, y ello se vuelve a poner de manifiesto nuevamente en la Comunicación de la Comisión al Parlamento Europeo y al Consejo, sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la Unión Europea y las

[36] La Comisión Europea, en su informe emitido en fecha 20 de octubre de 2004, SEC (2004) 1323, se basa en el emitido con anterioridad, en la primera evaluación que se realizó al respecto, mediante el Documento de Trabajo SEC (2002) 196, de fecha 13 de febrero de 2002, que fue respaldado posteriormente por sendos documentos de trabajo emitidos por parte del GT29 (puede consultarse en: http://ec.europa.eu/transparency/regdoc/rep/2/2002/ES/2-2002-196-ES-1-1.Pdf) [consultado el 20.08.2017].
En el informe objeto de citación en el cuerpo del texto, de 2004, ya la Comisión pone de relieve la falta de transparencia de las organizaciones estadounidenses que se adhieren al marco de cumplimiento por lo que se refiere, en particular, al cumplimiento de los estándares fijados para las políticas de privacidad, que dificultan, a su vez, la tarea de supervisión de las mismas por parte de las autoridades de control de Estados Unidos que tienen competencias sobre este asunto. Para mayor información, se ruega su consulta a través del siguiente enlace: http://ec.europa.eu/justice/policies/privacy/docs/adequacy/sec-2004-1323_en.pdf [consultado el 20.08.2017].

empresas establecidas en la misma, de fecha 27 de noviembre de 2013[37], cuando afirma, en relación con esta cuestión, el siguiente tenor literal: "Los progresos a este respecto han sido limitados. Desde el 1 de enero de 2009, el Departamento de Comercio evalúa la política de protección de la vida privada antes de renovar la certificación de puerto seguro de las entidades que deseen hacerlo –lo que debe hacerse anualmente. Sin embargo, es una evaluación limitada, ya que no se evalúan plenamente las prácticas reales de las entidades auto-certificadas, lo que haría mucho más fiable el procedimiento de auto-certificación".

No resulta una cuestión baladí señalar adicionalmente que a los anteriores principios enumerados se le han adicionado una serie de excepciones a su cumplimiento, tal y como podemos observar a través de la redacción introducida en la propia Decisión de la Comisión, de 26 de julio de 2000, objeto de análisis: "La adhesión a estos principios puede limitarse: a) cuando 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; c) por excepción o dispensa prevista en la Directiva o las normas de Derecho interno de los Estados miembros siempre que tal excepción o dispensa se aplique en contextos comparables"[38].

(iii) Cuestiones prácticas sucedidas durante su vigencia

A tenor de la evolución de la sociedad y de la proliferación de nuevas realidades y paradigmas digitales se han suscitado numerosas cuestiones prácticas sobre la aplicación de la Decisión de la Comisión que está siendo objeto de comentario. Entre otras, entiendo conveniente destacar, en primer término, el aumento exponencial de la cantidad de organizaciones estadounidenses que decidieron adherirse al Acuerdo de Puerto Seguro durante el período que comprende de 2004 a 2013, pasando de 400 en ese primer año a 3.246 en la última de las anualidades indicadas, según datos expresados por parte de la propia Comisión Europea[39].

En segundo término, podríamos aducir que, a la luz de las revelaciones desencadenadas por Edward Snowden a través del periódico británico *The Guardian*, en junio de 2013[40], acerca de las

[37] Comunicación de la Comisión al Parlamento Europeo y al Consejo, sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la Unión Europea y las empresas establecidas en la misma, de fecha 27 de noviembre de 2013 (COM (2013) 847 final). Puede consultarse en línea a través del siguiente enlace: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com(2013)0847_/com_com(2013)0847_es.pdf [consultado el 20.08.2017].

[38] No es óbice apuntar que esta agrupación de excepciones, que abusan de la utilización de conceptos jurídicos indeterminados, preocupaba a las autoridades europeas garantes sobre la materia, y ello fue también puesto de relieve por el propio GT29, a través de la Opinión 7/1999, de fecha 3 de diciembre de 1999, reseñada con anterioridad.

[39] Comunicación de la Comisión al Parlamento Europeo y al Consejo, sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la Unión Europea y las empresas establecidas en la misma, de fecha 27 de noviembre de 2013 (COM (2013) 847 final). Puede consultarse en línea a través del siguiente enlace: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com(2013)0847_/com_com(2013)0847_es.pdf [consultado el 20.08.2017].

[40] Para mayor información sobre esta cuestión, se ruega consultar el siguiente enlace: https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 [consultado el 20.08.2017].

operaciones de vigilancia masiva e indiscriminada llevadas a cabo por el Gobierno de los Estados Unidos a través de su Agencia de Seguridad Nacional (en adelante, NSA[41]), se pusieron de manifiesto las deficiencias normativas existentes en el marco que regulaba las transferencias internacionales de datos personales a territorio estadounidense.

En este mismo contexto, durante las alegaciones efectuadas por las organizaciones que podrían haber participado en las actividades de vigilancia masiva, se sucedieron adicionalmente las demandas que solicitaban la suspensión automática, y posterior revocación, del Acuerdo de Puerto Seguro, realizadas tanto por parte de determinados sectores sociales como por las propias autoridades de control de algunos Estados miembros[42].

Ante esta tesitura, el Gobierno de los Estados Unidos, en aquellos momentos liderado por el presidente Barack Obama, se vio obligado a admitir las filtraciones que se habían producido. En concreto, puso de manifiesto la existencia de varios "programas" de vigilancia masiva como, por ejemplo, sucedió, entre otros, con el programa acuñado bajo la denominación PRISM. Sobre ello tuvo ocasión de pronunciarse la Comisión Europea a través de sendas y rotundas declaraciones, afirmando literalmente al respecto que: "A lo largo de 2013, la información sobre la escala y el alcance de los programas estadounidenses de vigilancia han suscitado inquietudes sobre la continuidad de la protección de los datos personales transferidos a Estados Unidos con arreglo al marco de puerto seguro. Por ejemplo, aparentemente todas las empresas involucradas en el programa PRISM, y que conceden a las autoridades estadounidenses acceso a los datos almacenados y tratados en Estados Unidos, tienen el certificado de puerto seguro. Esto ha hecho de puerto seguro uno de los conductos a través de los cuales se da acceso a las autoridades de inteligencia estadounidenses para recopilar datos personales que han sido tratados inicialmente en la Unión Europea"[43].

Debe agregarse que las diversas agencias de inteligencia que intervenían en estas operaciones de vigilancia masiva, bajo las órdenes del Gobierno de los Estados Unidos, encontraban su habilitación normativa a través de la *Foreign Intelligence Surveillance Act*[44], denominada comúnmente bajo el acrónimo FISA –por sus siglas en inglés–, aprobada por el Congreso de Estados Unidos en 1978, que, mediante la creación de unos tribunales especiales, permitía que los mismos decidieran sobre la aprobación o denegación de las solicitudes del Gobierno estadounidense para realizar la

[41] La National Security Agency, también conocida habitualmente pos sus siglas en inglés, NSA, se podría definir como un órgano de inteligencia creado por parte del gobierno de los Estados Unidos de América, dependiente del Departamento de Defensa, que tiene como principal objetivo el análisis masivo de las comunicaciones, entendido el concepto en un sentido extensivo, con la intención de garantizar la protección y salvaguarda de los intereses gubernamentales.

[42] Resolución del Parlamento Europeo, de fecha, 4 de julio de 2013, sobre el programa de vigilancia de la Agencia Nacional de Seguridad de Estados Unidos, los organismos de vigilancia en varios Estados miembros y su impacto en la vida privada de los ciudadanos de la Unión Europea (2013/2682 (RSP)). En línea: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2013 0322+0+DOC+PDF+V0//EN [consultado el 20.08.2017].

[43] Comunicación de la Comisión al Parlamento Europeo y al Consejo, sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la Unión Europea y las empresas establecidas en la misma, de fecha 27 de noviembre de 2013 (COM (2013) 847 final). Puede consultarse en línea a través del siguiente enlace: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com(2013)0847_/com_com(2013)0847_es.pdf [consultado el 20.08.2017].

[44] Para mayor información sobre esta cuestión, se ruega consultar el texto legislativo a través del siguiente enlace: https://www.law.cornell.edu/uscode/text/50/chapter-36 [consultado el 20.08.2017].

intervención de las comunicaciones de ciudadanos u organismos extranjeros por motivos de seguridad nacional.

A este respecto, conviene señalar también que la Sección 215 de la *Patriot Act*[45] permitía que las agencias de inteligencia norteamericanas solicitasen a los tribunales especiales, creados bajo el amparo de la FISA, una orden –con carácter secreto– que obligaba a las organizaciones destinatarias a entregar *any tangible things*, siempre que las mismas pudieran ser *relevant to an authorised preliminary or full investigation to obtain foreign intelligence information not concerning a US person*. Asimismo, dicha Sección habilita a las referidas agencias para que puedan obtener cualquier tipo de información sobre la tipología de clientes de una determinada compañía con el argumento basado en *to protect against international terrorism or clandestine intelligence activities*.

Asimismo, y de conformidad con lo que se viene comentando, podríamos llegar a entender que el hecho de realizar una monitorización, seguimiento y evaluación de las comunicaciones como el que se venía realizando por parte de las autoridades norteamericanas podría llegar a resultar contrario al contenido estipulado en la Cuarta Enmienda reseñada con anterioridad, pero este punto ya fue objeto de análisis por parte de la U. S. District & Bankruptcy Court for the District of Columbia, al señalar, en el *Memorandum Opinion* sobre la Civil Action N.º 13-0851 (RJL)[46], de fecha 16 de diciembre de 2013, que aunque el Gobierno estadounidense sostenga, como principal argumento, que las escuchas telefónicas estarían amparadas por el precedente sentado mediante el pronunciamiento que realizó el Tribunal Supremo de los Estados Unidos en el caso Smith v. Maryland, 442 US 73 5 (1979)[47], dado que estableció que no se otorgaba una expectativa razonable de privacidad respecto de los datos personales que se transmiten a las operadoras de telecomunicaciones.

Sin embargo, la susodicha U. S. District & Bankruptcy Court for the District of Columbia, a través del juez Richard J. Leon, que suscribe el documento, mantiene que la situación que se analiza en este caso concreto, relativo a uno de los programas de vigilancia masiva orquestados por la NSA –denominado Bulk Telephony Metadata Program–[48], no podía ser susceptible de realizar un ejercicio de analogía con el caso Smith v. Maryland, pues los paradigmas de los que se partía eran antagónicamente diferentes, afirmando al respecto el siguiente tenor literal: *"Just as the Court in Knotts did not address the kind of surveillance used to track Jones, the Court in Smith was not confronted with the NSA's Bulk Telephony Metadata Program. Nor could the Court in 1979 have ever imagined*

[45] Para mayor información sobre esta cuestión, se ruega consultar el texto legislativo a través del siguiente enlace: https://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf [consultado el 20.08.2017].

[46] *Memorandum of Opinion*, emitido por parte de la U. S. District & Bankruptcy Court for the District of Columbia, en fecha 16 de diciembre de 2013, en sede de la Civil Action N.º 13-0851 (RJL). En línea a través del siguiente enlace: https://online.wsj.com/public/resources/documents/JudgeLeonNSAopinion12162013.pdf [consultado el 20.08.2017].

[47] Para mayor información sobre este caso, puede profundizarse su contenido jurídico a través del siguiente enlace: https://www.oyez.org/cases/1978/78-5374 [consultado el 20.08.2017].

[48] Se trataba de un programa de vigilancia arbitrado por la NSA para obtener todos los metadatos de las comunicaciones objeto de intervención. Véase, para mayor información, el siguiente enlace: http://www.newyorker.com/news/daily-comment/the-metadata-program-in-eleven-documents [consultado el 20.08.2017]. No obstante, supuestamente, la aludida agencia de inteligencia habría dejado de utilizar el referido programa a finales de 2015. Véase, para mayor información, el siguiente enlace: https://www.lawfareblog.com/nsa-ends-bulk-collection-telephony-metadata-under-section-215 [consultado el 20.08.2017].

how the citizens of 2013 would interact with their phones. For the many reasons discussed below, I am convinced that the surveillance program now before me is so different from a simple pen register that Smith is of little value in assessing whether the Bulk Telephony Metadata Program constitutes a Fourth Amendment search. To the contrary, for the following reasons, I believe that bulk telephony metadata collection and analysis almost certainly does violate a reasonable expectation of privacy".

Teniendo en cuenta lo anterior, resulta ilustrativo apuntar, a título anecdótico, el artículo publicado en el diario británico *The Economist*, en fecha 15 de junio de 2013, titulado "Surveillance: Look who's listening"[49], el cual comentaba sarcásticamente que las autoridades estadounidenses parecían creer que la obtención de registros de cada llamada telefónica efectuada en Estados Unidos resultaba susceptible de ser considerada relevante para una investigación o un baluarte esencial de la lucha que efectuaba el referido país contra el terrorismo internacional.

Una vez realizado este breve apunte, y siguiendo con el hilo explicativo, debe mantenerse que el proceso de autorización descrito en el marco de la FISA, *a priori*, estaba supervisado y controlado a través de distintos operadores. Por un lado, encontramos a los tribunales especialmente designados a través de la susodicha legislación, con el soporte del Congreso de los Estados Unidos (que emitía dos informes al año sobre cada asunto tratado) y, por otro lado, podemos citar la participación de los inspectores generales independientes que, bajo el principio de mínima intervención, intentaban salvaguardar y preservar los derechos de los afectados ante la recogida masiva de sus datos de carácter personal.

Consideración, esta última, que ha quedado totalmente desmentida, por causa de las filtraciones a las que hemos aludido con anterioridad, y que ponen de manifiesto una total ausencia de control por parte de las autoridades gubernamentales norteamericanas, en detrimento de la (des) protección de los derechos consagrados por la regulación europea a sus ciudadanos, violación de la que las autoridades comunitarias fueron totalmente conocedoras.

Tal es así que, en tercer y último término, debe subrayarse que la Comisión Europea, el 27 de noviembre de 2013, reabrió el diálogo con las autoridades de Estados Unidos mediante una serie de comunicaciones efectuadas al Parlamento Europeo y al Consejo de la Unión Europea, las cuales han sido colacionadas a lo largo del presente texto[50], que iban intencionadas a reafirmar la alianza estratégica que unía a ambos territorios, destacando la importancia fundamental de los flujos de datos transatlánticos para el comercio, la aplicación de la legislación vigente y las políticas nacionales, pero reconociendo, a su vez, que las revelaciones efectuadas por el Sr. Snowden habían dañado la confianza de la Unión Europea en el Acuerdo de Puerto Seguro y que la misma debería de ser reconstruida y fortalecida. En las mencionadas comunicaciones, la Comi-

[49] Para mayor información, puede consultarse el artículo a través del siguiente enlace: https://www.economist.com/news/briefing/21579473-americas-national-security-agency-collects-more-information-most-people-thought-will [consultado el 20.08.2017].

[50] Comunicación de la Comisión al Parlamento Europeo y al Consejo, sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la Unión Europea y las empresas establecidas en la misma, de fecha 27 de noviembre de 2013 (COM (2013) 847 final). Puede consultarse en línea a través del siguiente enlace: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com(2013)0847_/com_com(2013)0847_es.pdf [consultado el 20.08.2017].

sión efectuó trece recomendaciones, que tenían como principal objetivo subsanar las debilidades que habían sido puestas de manifiesto sobre el Acuerdo de Puerto Seguro para que el mismo pudiera seguir siendo un mecanismo eficaz que permitiera el intercambio transatlántico de datos personales.

Las recomendaciones se centraron principalmente en cuatro grandes líneas: **(i) transparencia:** las políticas de privacidad de las organizaciones norteamericanas adheridas al marco de cumplimiento deberían de ser públicas en sus correspondientes sitios web, redactadas con un lenguaje claro y sencillo, con vínculos al sitio web del Departamento de Comercio donde aparezca el listado de todas las organizaciones adheridas y, al mismo tiempo, especificando las condiciones en las cuales se efectúan las subcontrataciones para la prestación de determinados servicios por lo que concierne a la protección de los datos personales de los afectados; **(ii) recursos:** las políticas de privacidad deberán de incluir enlaces a terceros que se encarguen de la solución extrajudicial de litigios, los cuales deberán de ser asequibles y ser fácilmente disponibles, dado que el Departamento de Comercio velará por su cumplimiento; **(iii) aplicación:** se articularán inspecciones de oficio para verificar el nivel de cumplimiento de las entidades adheridas, así como se efectuarán investigaciones cuando se tengan indicios de incumplimientos o se hayan recibido denuncias al respecto, debiendo informar a las autoridades comunitarias siempre que ello resulte necesario; **(iv) acceso por parte de las autoridades estadounidenses:** las políticas de privacidad explicarán de manera detallada cómo la legislación norteamericana permite el acceso a los datos personales transferidos en el marco del Acuerdo de Puerto Seguro, teniendo en cuenta que las excepciones previstas serán utilizadas únicamente cuando resulte estrictamente necesario.

Sobre la base de las recomendaciones esbozadas, las autoridades comunitarias realizaron intensas negociaciones, hasta que, en junio de 2014, Viviane Reding efectuó unas declaraciones[51] que actualizaban la información de la que hasta el momento se disponía, donde expuso que el Departamento de Comercio de los Estados Unidos había aceptado doce de las trece recomendaciones, estableciendo el siguiente tenor literal al respecto: "*What exactly is the 'sticking point' in the negotiations with the U.S. and will the Americans play for time with the European Commission's current mandate coming to an end? We have an institutional continuity. Just because there is a change in Commissioner doesn't mean there will be a change in policy. Everything a Commissioner does is backed by the College. On Safe Harbor, it is the primary responsibility of the Commission to operate on this point. I told you, out of 13 points, 12 have been agreed, the 13th on is the National security exception – for me it is an exception not a rule. We have a problem of definition here. It should be an exception not a hoover. This must be clarified before we can give our agreement to Safe Harbor – and if I say 'we' I speak in the name of my institution*".

[51] Nota de prensa efectuada por la entonces vicepresidenta de la Comisión Europea, Viviane Reding, en fecha 6 de junio 2014, sobre las negociaciones del Acuerdo de Puerto Seguro, a la luz de las revelaciones sobre la vigilancia masiva realizadas por E. Snowden. En línea: http://europa.eu/rapid/press-release_SPEECH-14-431_en.htm [consultado el 20.08.2017].

(iv) Sentencia del Tribunal de Justicia de la Unión Europea, de 6 de octubre de 2015 (Asunto C-362/14) – Schrems[52]

Cabe iniciar la explicación del presente apartado haciendo una breve introducción sobre el supuesto de hecho que antecede la presente decisión judicial. El Sr. Maximillian Schrems, estudiante austríaco de derecho y con residencia habitual en ese mismo país, en fecha 25 de junio de 2013, decide instar una denuncia ante el Data Protection Comissioner (equivalente a la autoridad nacional de protección de datos irlandesa), solicitando la suspensión de las transferencias internacionales de sus datos personales de Facebook Ireland a los Estados Unidos, afirmando que esta última mercantil citada –considerada como responsable del tratamiento– ya no gozaba de mecanismos que legitimaran las transferencias transatlánticas de sus datos de carácter personal, puesto que había quedado totalmente demostrado, fruto de las revelaciones efectuadas por E. Snowden, el acceso indiscriminado del que estaban gozando las agencias de inteligencia estadounidenses a los datos personales de ciudadanos europeos.

Sin embargo, el comisionado irlandés desestimó la denuncia sobre la base de que la Comisión Europea ya había determinado, con anterioridad a la denuncia presentada, la viabilidad del Acuerdo de Puerto Seguro y que, por lo tanto, no podía impugnar la validez de la decisión adoptada por la Comisión Europea. Ello no convenció al Sr. Schrems, por lo que optó por la posibilidad de acudir al Tribunal Supremo de Irlanda, con la intención de que la decisión adoptada por el comisionado irlandés fuera objeto de revisión en relación con la viabilidad del nivel de protección adecuado que hasta esa fecha gozaban los Estados Unidos de América.

En este contexto, el Tribunal Supremo de Irlanda consideró que la *quaestio litis* concernía a una materia que debía de sustanciarse mediante los órdenes jurisdiccionales comunitarios. Es por este motivo por el que decide suspender el procedimiento nacional para plantear una cuestión prejudicial al Tribunal de Justicia de la Unión Europea sobre dos puntos. Por un lado, sobre si una autoridad de control nacional en materia de protección de datos, aunque tenga comprobado que en un tercer país no se garantiza un nivel de protección adecuado de los datos personales recabados, está vinculada, en su totalidad, por las decisiones que hubiera emitido la Comisión Europea, en el presente caso concreto, se trataba de lo relativo a la Decisión de 26 de julio de 2000, analizada y comentada en los anteriores epígrafes.

Y, por otro lado, en el supuesto de que no existiera una vinculación directa, se planteó la cuestión sobre si una autoridad de control nacional en materia de protección de datos personales podría realizar sus propias investigaciones sobre ese concreto asunto como consecuencia de la aparición de nuevos hechos noticiables que recomendaban la revisión de la Decisión de la Comisión de fecha 26 de julio de 2000.

[52] Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 6 de octubre de 2015, en el asunto C-362/14, que tiene por objeto una petición de decisión prejudicial planteada, con arreglo al artículo 267 TFUE, por la High Court (Irlanda), mediante resolución de 17 de julio de 2014, recibida en el Tribunal de Justicia el 25 de julio de 2014, en el procedimiento entre Maximillian Schrems y el Data Protection Commissioner, con la intervención de Digital Rights Ireland Ltd. En línea. http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=ES [consultado el 20.08.2017].

Ante esta situación, el Tribunal de Justicia de la Unión Europea celebró su primera y única audiencia pública sobre este asunto el 24 de marzo de 2015 para posteriormente, en fecha 6 de octubre de 2015, hacer público su pronunciamiento, declarando la invalidez de la Decisión de la Comisión, de fecha 26 de julio de 2000, basándose en una serie de fundamentos jurídicos, los cuales serán objeto de comentario en las siguientes líneas de redacción.

En primer lugar, cabe apuntar la advertencia central que se reproduce en el texto de la sentencia respecto de la obligatoriedad a la que están sometidos los Estados miembros y, por ende, sus respectivas autoridades nacionales, a dar cumplimiento de los pronunciamientos que se emitan por parte de las organismos europeos, en este caso, las decisiones emitidas por parte de la Comisión Europea, al amparo de las facultades que le reconoce el artículo 25.6 de la Directiva 95/46/CE, dado que, como consecuencia del artículo 28.4 del Tratado de Funcionamiento de la Unión Europea[53], las decisiones que adopte la Comisión tendrán carácter vinculante para los Estados miembros, quienes deberán de articular los medios que resulten necesarios para darle el debido cumplimiento, siempre que las mismas no hayan sido previamente declaradas inválidas por parte de los órganos jurisdiccionales correspondientes.

En segundo lugar, se determina la ausencia de efectividad del mecanismo de autocertificación que propugnaba el artículo 1 de la Decisión de la Comisión, de fecha 26 de julio de 2000, dado que los principios establecidos en el citado Acuerdo de Puerto Seguro eran únicamente aplicables a las entidades que hubieran decidido voluntariamente someterse a ellos y que en ningún caso los propios poderes públicos estadounidenses optaron por la sumisión a los mismos, y aún el problema se intensifica si tenemos en cuenta que no se articulaban procedimientos legislativos que garantizasen el cumplimiento de los referidos principios[54].

A este respecto, afirma la sentencia, en el apartado 81, que: “Aunque el recurso por un tercer país a un sistema de auto-certificación no es por sí mismo contrario a la exigencia enunciada en el artículo 25, apartado 6, de la Directiva 95/46 de que el tercer país considerado garantice un nivel de protección adecuado ‘a la vista de su legislación interna o de sus compromisos internacionales’, la fiabilidad de ese sistema en relación con dicha exigencia descansa, en esencia, en el establecimiento de mecanismos eficaces de detección y de control que permitan identificar y sancionar en la práctica las posibles infracciones de las reglas que garantizan la protección de los derechos fundamentales, en especial del derecho al respeto de la vida privada y del derecho a la protección de los datos personales”.

En tercer lugar, conviene señalar que, según el Tribunal de Justicia de la Unión Europea (en adelante, TJUE), la Decisión de la Comisión, de fecha 26 de julio de 2000, identifica la primacía de determinados aspectos consagrados por el ordenamiento jurídico de Estados Unidos, tales como las “exigencias de seguridad nacional, interés públicos y el cumplimiento de la ley –estadouniden-

[53] Artículo 28 del Tratado de Funcionamiento de la Unión Europea. En línea: http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:12012E291 [consultado el 20.08.2017].

[54] Apartados 82 y 83 de la sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 6 de octubre de 2015, en el asunto C-362/14, reseñada con anterioridad.

se", sobre los principios reflejados en el Acuerdo de Puerto Seguro, facilitándose así la injerencia en el derecho fundamental a la protección de los datos personales sin la observancia de las debidas garantías, tal y como ha quedado demostrado a través del análisis que efectúa la Comisión sobre la aplicación de las disposiciones contenidas en el susodicho marco normativo[55].

Es por ello por lo que se hace preciso, a título ilustrativo, aportar la literalidad de las declaraciones contenidas en el texto jurisprudencial cuando se apunta que: "En lo que atañe al nivel de protección de las libertades y derechos fundamentales garantizado en la Unión, según reiterada jurisprudencia del Tribunal de Justicia, una normativa de esta que haga posible una injerencia en los derechos fundamentales garantizados por los artículos 7 y 8 de la Carta debe contener reglas claras y precisas que regulen el alcance y la aplicación de una medida e impongan unas exigencias mínimas, de modo que las personas cuyos datos personales resulten afectados dispongan de garantías suficientes que permitan proteger eficazmente sus datos personales contra los riesgos de abuso y contra cualquier acceso o utilización ilícitos de estos"[56].

Estableciéndose al respecto que la protección del derecho fundamental al respeto de la privacidad y, por ende, a los datos de carácter personal, únicamente puede soportar excepciones cuando estas no excedan de lo estrictamente necesario, por lo que la sentencia del TJUE determina 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 […]. En particular, se debe considerar que una normativa que permite a las autoridades públicas acceder de forma generalizada al contenido de las comunicaciones electrónicas lesiona el contenido esencial del derecho fundamental al respeto de la vida privada garantizado por el artículo 7 de la Carta"[57].

En cuarto y último lugar, podemos aducir que el TJUE, ante esta situación, concluye que las autoridades europeas con competencias sobre la materia –especialmente, la Comisión Europea–, no efectuaron las comprobaciones suficientes que llegaran a determinar con exactitud que los Estados Unidos de América gozaban de un nivel de protección adecuado, y máxime si tenemos en cuenta que, además de dotar de mecanismos de tutela inservibles a los afectados, se optó por dificultar el ejercicio de ciertas facultades a las autoridades nacionales de los Estados miembros, incumpliendo, en su totalidad, las vicisitudes contenidas en el artículo 25.6 de la Directiva 95/46/CE, trayendo como último resultado la invalidez del Acuerdo de Puerto Seguro remarcada *ut supra*.

[55] Apartado 90 de la sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 6 de octubre de 2015, en el asunto C-362/14, reseñada con anterioridad.

[56] Apartado 91 de la sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 6 de octubre de 2015, en el asunto C-362/14, reseñada con anterioridad.

[57] Apartados 93 y 94 de la sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 6 de octubre de 2015, en el asunto C-362/14, reseñada con anterioridad.

(v) Implicaciones de la sentencia Schrems para las transferencias internacionales de datos personales a los Estados Unidos de América

En el marco de este contexto, y ante la inseguridad jurídica generada por la invalidez de la Decisión de la Comisión que hasta la fecha hacía viables las transferencias internacionales de datos a Estados Unidos, el Grupo de Trabajo del Artículo 29, en fecha 16 de octubre de 2015, realizó una nota de prensa[58] que ponía de manifiesto, por un lado, la necesidad de realizar un llamamiento, en primer término, a los Estados miembros y a las autoridades nacionales de protección de datos para que encontraran una posición unánime en la aplicación de la sentencia Schrems[59] y, en segundo término, a las autoridades comunitarias para que empezaran las negociaciones con las autoridades estadounidenses en aras de encontrar una alternativa que permitiera seguir operando con los flujos de datos personales transfronterizos, pero esta vez con la adopción de mecanismos claros y vinculantes que asegurasen la salvaguarda de los derechos fundamentales, en especial del relativo a la protección de los datos personales.

Y, por otro lado, la referenciada nota de prensa hace especial hincapié en la necesidad de encontrar soluciones alternativas para realizar las transferencias internacionales de datos a los Estados Unidos, dado que el marco jurídico que las sustentaba había devenido inválido, cosa que en la práctica, para las organizaciones, implicó que, por ejemplo, en España, aunque la Agencia Española de Protección de Datos anunció que no iniciaría actuaciones inspectoras y sancionadoras en este sentido[60], se buscasen otras opciones para seguir con la misma operativa de negocio que hasta la fecha se venía siguiendo, tales como las cláusulas contractuales tipo adoptadas por las Decisiones de la Comisión Europea 2001/497/CE, 2004/915/CE y 2010/87/UE, las normas corporativas vinculantes (BCR) o garantizar que la transferencia en cuestión se ajustase a alguna de las excepciones contenidas en el artículo 26.1 de la Directiva 95/46/CE (o, en el caso español, recogidas en el artículo 34 de la LOPD).

[58] Declaración del GT29, de fecha 16 de octubre de 2015, relativa a las implicaciones de la sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 6 de octubre de 2015, en el asunto C-362/14, reseñada con anterioridad. En línea: a través del siguiente enlace de consulta electrónica: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf [consultado el 24.08.2017].

[59] A este respecto, se recomienda consultar la nota de prensa publicada en la página web oficial de la Agencia Española de Protección de Datos, en fecha 19 de octubre de 2015, donde se anuncia que *"las Autoridades europeas de Protección de Datos publican una declaración conjunta en relación con la aplicación de la sentencia del TJUE sobre el Puerto Seguro"*. En línea, a través del siguiente enlace de consulta electrónica: https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2015/notas_prensa/news/2015_10_19-ides-idphp.php#Actuaci%C3%B3n%20conjunta [consultado el 24.08.2017].

[60] Para mayor información, se ruega consultar la comunicación oficial que remitió la Agencia Española de Protección de Datos a los responsables, y que hizo pública en su página web, en fecha 29 de octubre de 2015, pudiéndose consultar la misma a través del siguiente enlace de consulta electrónica: https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/common/Comunicacion_responsables_-_Puerto_Seguro.pdf [consultado el 24.08.2017].

3. NUEVO PARADIGMA PARA LAS TRANSFERENCIAS INTERNACIONALES DE DATOS A ESTADOS UNIDOS. EL NOVEDOSO *EU-U. S. PRIVACY SHIELD FRAMEWORK*

(i) Antecedentes

A principios de 2016, concretamente el 29 de febrero de ese mismo año, y transcurridos más de dos años desde el inicio de las negociaciones con el Departamento de Comercio de los Estados Unidos, la Comisión hizo público el proyecto de decisión sobre el nuevo marco regulador de las transferencias internacionales entre ambos territorios, el cual fue acuñado bajo la denominación *EU-U. S. Privacy Shield framework*[61].

Posteriormente, entre los meses de marzo y julio de 2016, se dio traslado del texto a varios organismos comunitarios para que realizaran los comentarios que considerasen oportunos, en concreto, el Parlamento Europeo y el GT29 realizaron una serie de pronunciamientos[62] que abogaban por la introducción de mejoras en ciertos puntos, tales como los periodos de retención de los datos de carácter personal, así como las ulteriores transferencias de los mismos.

A mayor abundamiento, cabe recordar que el GT29 emitió una declaración preliminar[63], en fecha 3 de febrero de 2016 (es decir, con anterioridad a que la documentación se hubiera divulgado *erga omnes*), donde ponía de manifiesto la satisfacción sobre las conclusiones que se habían alcanzado en el seno de las arduas negociaciones entre la Unión Europea y los EE. UU. En este mismo documento se identificaron cuatro garantías esenciales a las que se deberían dar cumplimiento cuando las agencias de inteligencia pretendieran acceder a datos de carácter personal de ciudadanos europeos, las cuales pueden detallarse brevemente en que: **(i)** el tratamiento de los datos personales se sustentará bajo los principios de claridad, precisión y accesibilidad; **(ii)** se respetarán los principios de necesidad y proporcionalidad cuando se acceda a datos personales; **(iii)** existirán mecanismos de supervisión independientes; y **(iv)** se facilitarán a los interesados mecanismos que ofrezcan una correcta tutela de sus derechos. Finalmente, en fecha 12 de julio de 2016, la Comisión Europea, mediante nota de prensa[64], hizo pública la adopción del Acuerdo sobre el Escudo de Privacidad UE-EE. UU., que constituye el marco normativo que posibilita las transferencias internacionales de datos personales de ciudadanos europeos hacia el mencionado territorio.

[61] Decisión de ejecución (UE), n.º 2016/1250, de la Comisión, de fecha 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. [notificada con el número C-(2016) 4176]. Puede consultarse a través del siguiente enlace: http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016D1250&from=EN [consultado el 24.08.2017].

[62] "Opinion 01/2016, on the EU - U.S. Privacy Shield draft adequacy decision", emitida por el GT29 en fecha 13 de abril de 2016. Puede consultarse en línea a través del siguiente enlace: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf [consultado el 24.08.2017].

[63] Declaración del GT29, de fecha 3 de febrero de 2016, relativa a las consecuencias de la sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), de 6 de octubre de 2015, en el asunto C-362/14, reseñada con anterioridad. En línea: a través del siguiente enlace de consulta: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf [consultado el 24.08.2017].

[64] Nota de prensa efectuada por la Comisión Europea, en fecha 12 de julio 2016, sobre la adopción del Acuerdo sobre Escudo de Privacidad UE-EE. UU. En línea http://europa.eu/rapid/press-release_IP-16-2461_es.htm [consultado el 24.08.2017].

(ii) Contenido

El contenido y estructura de la Decisión de ejecución (UE), n.º 2016/1250, de la Comisión, de fecha 12 de julio de 2016, se compone, en primer lugar, por ciento cincuenta y cinco considerandos iniciales, en segundo lugar, por seis artículos que intentan plasmar el calado jurídico de la norma para, finalmente en el último tramo de la misma, incorporar una serie de anexos, que llegan hasta el número séptimo, y que tienen como principal objetivo intentar arrojar luz y facilitar la aplicabilidad práctica del texto de la Decisión.

Siguiendo con los precedentes sentados por el anterior acuerdo, el marco normativo sobre el escudo de privacidad parte también de un mecanismo de autocertificación que debe de notificarse ante el Departamento de Comercio de los Estados Unidos, mediante la adhesión al cumplimiento de una serie de principios que vienen consagrados en el Anexo II de la Decisión, los cuales se estructuran, a grandes rasgos, en siete principios generales y dieciséis que tienen carácter complementario.

En este mismo sentido, el presente apartado no pretende resultar en un tratamiento pormenorizado sobre el contenido del nuevo marco normativo sobre el escudo de privacidad, dado que, si el mismo se efectuase, extendería en demasía el ámbito de lo aquí pretendido, sino que su objetivo radica en poner de manifiesto aquellas cuestiones más relevantes que difieren del texto de su antecesor, el Acuerdo de Puerto Seguro, que ha sido objeto de comentario en las anteriores líneas. Para ello, procederemos a enumerar brevemente aquellas consideraciones que destacan en la reciente regulación, por su mayor enjundia.

En primer lugar, encontramos el **principio de notificación**, que requiere que las organizaciones estadounidenses que se adhieran al nuevo marco normativo proporcionen información más específica en sus respectivas políticas de privacidad. En la práctica, ello ya venía sucediendo con el anterior Acuerdo de Puerto Seguro, pero a muy alto nivel, por lo que se ha optado por detallar específicamente los requisitos que esa concreta política deberá de cumplir, introduciendo novedades como la necesidad de incluir un enlace electrónico al formulario de presentación de quejas y reclamaciones para la resolución extrajudicial de controversias o la obligatoriedad de reconocer la responsabilidad en los supuestos de transferencias ulteriores a terceros.

En relación con lo anterior, sería conveniente advertir que puede resultar peligroso, en ocasiones, incurrir en un exceso de detalle, dado que ello podría entrar en conflicto con los principios generales por los que aboga el propio texto de la Decisión, centrados en la utilización de un lenguaje sencillo, claro y visible. Es por ello por lo que las organizaciones, en el momento en que opten por su redacción, deberán tener en cuenta estas consideraciones para no entrar en colisión con otros puntos esenciales del texto normativo.

En segundo lugar, podemos visualizar el **principio de opción**, que no introduce novedades significativas respecto de lo que se venía manteniendo en el anterior texto de la Comisión, ofreciendo a los interesados la posibilidad de decidir si sus datos personales pueden ser cedidos a terceros o si pueden ser utilizados para finalidades distintas para las que fueron originalmente recabados. Resulta importante destacar la introducción de una excepción ante el cumplimiento de este princi-

pio general, que radica en que cuando ese tercero actúe como agente –es decir, bajo la condición de encargado del tratamiento–[65], no será preciso ofrecer a los interesados ese derecho de opción, pero, sin embargo, la organización quedará obligada a suscribir un contrato con ese tercero donde se delimiten las instrucciones que le establezca al respecto como responsable del tratamiento.

En tercer lugar, cabe identificar el denominado **principio de responsabilidad "por una transferencia ulterior"**, que incorpora nuevas obligaciones para las organizaciones en detrimento de lo que establecía con anterioridad el Acuerdo de Puerto Seguro, destacándose al respecto que su contenido radica esencialmente en la protección de cualquier transferencia o comunicación de datos personales que se efectúe con posterioridad a otro responsable o encargado del tratamiento, pudiéndose realizar únicamente en determinados supuestos y siempre que medie la existencia de un vínculo contractual previo donde se estipule el cumplimiento de todos los principios reflejados en el marco normativo sobre el escudo de privacidad y, especialmente, el de proporcionar un nivel de protección adecuado.

La obligación contractual a la que se refiere este principio se asemeja a las diversas obligaciones estipuladas en el RGPD, dado que el responsable del tratamiento debe de mantener un deber de diligencia en la elección del encargado del tratamiento con la intención de que este último ofrezca garantías suficientes respecto de la implementación y mantenimiento de las medidas técnicas y organizativas apropiadas, garantizando, al mismo tiempo, la correcta tutela de los derechos de los afectados.

En particular, se ha creído conveniente reproducir la literalidad que aporta el considerando 81[66] al respecto: "El tratamiento por un encargado debe regirse por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros que vincule al encargado con el responsable, que fije el objeto y la duración del tratamiento la naturaleza y fines del tratamiento, el tipo de datos personales y las categorías de interesados, habida cuenta de las funciones y responsabilidades específicas del encargado en el contexto del tratamiento que ha de llevarse a cabo y del riesgo para los derechos y libertades del interesado. El responsable y el encargado pueden optar por basarse en un contrato individual o en cláusulas contractuales tipo que adopte directamente la Comisión o que primero adopte una autoridad de control de conformidad con el mecanismo de coherencia y posteriormente la Comisión. Una vez finalizado el tratamiento por cuenta del responsable, el encargado debe, a elección de aquel, devolver o suprimir los datos personales, salvo que el Derecho de la Unión o de los Estados miembros aplicable al encargado del tratamiento obligue a conservar los datos".

[65] Se recomienda, a título ilustrativo, revisar el contenido del considerando n.º 14 de Decisión de ejecución (UE), n.º 2016/1250, de la Comisión, de fecha 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. [notificada con el número C-(2016) 4176].

[66] Se recomienda visualizar la completitud del considerando n.º 80 del 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). En línea: https://www.boe.es/doue/2016/119/L00001-00088.pdf [consultado el 24.08.2017].

En cuarto lugar, advertimos el **principio de seguridad**, que mantiene el mismo redactado que el introducido en el anterior Acuerdo de Puerto Seguro, abogando por que las organizaciones que se encargan de recabar datos de carácter personal apliquen todas las precauciones necesarias que permitan evitar su pérdida, uso indebido, acceso no autorizado, divulgación, alteración o destrucción. Sin embargo, resulta sorprendente que se haya optado por un redactado tan amplio, en comparación con los restantes principios que hemos ido comentando a lo largo de los anteriores párrafos, que se caracterizan por la especificación y exactitud de las obligaciones que los mismos contemplan.

Resulta esencial comparar este aspecto con la mención que se contiene al respecto en el RGPD, cuando el mismo se hace eco de las medidas técnicas y organizativas que se deberán de implementar para la correcta protección y salvaguarda de los datos personales de los afectados, donde se hace uso de innumerables conceptos jurídicos indeterminados[67] que dificultan, en la práctica, la operativa de negocios de las organizaciones, dado que no se han facilitado orientaciones para que las mismas puedan dar cumplimiento a estos requisitos normativos, máxime si tenemos en cuenta que, a día de hoy, no se ha establecido ningún pronunciamiento claro entre la "supuesta" utilidad de marcos de referencia en materia de seguridad de la información, como podríamos citar, a título de ejemplo, la Norma ISO 27000 o el estándar COBIT, y su alineamiento con las disposiciones contenidas en el referenciado RGPD.

En quinto lugar, identificamos el **principio de integridad de los datos y la limitación de la finalidad** para la que son destinados, que mantiene las mismas obligaciones que el ya reiterado, Acuerdo de Puerto Seguro, haciendo hincapié en la necesidad de que las organizaciones que se adhieran al nuevo marco normativo deberán de adoptar medidas razonables que aseguren la utilización de los datos personales de conformidad con las finalidades para las que fueron recabados, es decir, deben de ser pertinentes para el uso previsto y la información contenida deberá ser precisa, completa y actualizada, todo ello durante el período que comprenda su conservación.

A este respecto, se añade explícitamente que cualquier organización que tenga acceso a estos datos personales deberá de adherirse al cumplimiento de los principios reflejados en el marco normativo sobre el escudo de privacidad, independientemente de que, una vez que deje de intervenir en el tratamiento de los mismos, decida retirarse del mismo. Ello va en consonancia con el espíritu de redacción del texto de la Decisión, que aboga por la protección de los datos de carácter personal durante todo el flujo de su vida, en especial cuando los mismos son destinados a terceros, lo cual obedece a las reiteradas quejas que se han sucedido tradicionalmente sobre esta cuestión, y que también el RGPD toma especialmente en consideración.

En sexto lugar, apreciamos el **principio de acceso**, que conserva un contenido similar al que fue objeto de introducción en la anterior Decisión de la Comisión, estableciéndose al respecto el

[67] Se recomienda realizar la lectura del artículo 32, párrafo primero, del 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). En línea: https://www.boe.es/doue/2016/119/L00001-00088.pdf [consultado el 24.08.2017].

siguiente tenor literal: "Los particulares deberán tener acceso a la información personal que las entidades tengan sobre ellos y poder corregir, modificar o suprimir dicha información si resultase inexacta, o haya sido tratada infringiendo los principios, excepto en dos casos: cuando permitir el acceso suponga una carga o dispendio desproporcionado en relación con los riesgos que el asunto en cuestión conlleve para la vida privada de la persona, o cuando puedan vulnerarse los derechos de otras personas".

Y, por último, en séptimo lugar, cabe apuntar la existencia del **principio de recurso, aplicación y responsabilidad**, que se ha visto ampliado significativamente respecto de lo que establecía con anterioridad el Acuerdo de Puerto Seguro y se encarga de establecer la obligatoriedad, para las organizaciones adheridas, de implementar mecanismos para los interesados que garanticen la correcta y efectiva tutela de sus derechos. Para ello se ha optado por articular una diversidad de procedimientos, tales como: **(i)** la asunción de responsabilidad por la propia organización afectada y adherida al acuerdo, que deberá de resolver en un plazo máximo de 45 días; **(ii)** la posibilidad de presentación de quejas y reclamaciones ante las propias autoridades nacionales de protección de datos de los Estados miembros o, en su defecto, ante el Departamento de Comercio estadounidense (a través de las distintas instituciones que estén designadas a tal efecto; *a priori*, ello se realizará a través de la Federal Trade Comission[68]), debido a que los susodichos órganos quedan obligados a colaborar para investigar y resolver las quejas o reclamaciones que puedan interponerse por parte de los ciudadanos europeos; **(iii)** la opción de acudir a un sistema extrajudicial de resolución de litigios, que deberá de tener carácter gratuito y **(iv)** con carácter subsidiario, en el supuesto de que no se haya resuelto la controversia por ninguna de las anteriores vías, se ha dejado abierta la posibilidad de acudir ante un procedimiento arbitral.

(iii) Valoraciones

Todo ello deberá de ser interpretado en su conjunto a través de los restantes principios complementarios que forman parte del Anexo II de la Decisión de ejecución (UE), n.º 2016/1250, y que tienen como objetivo principal intentar ayudar y orientar en la aplicación de los principios generales enumerados con anterioridad. No obstante, deberemos esperar para evaluar la efectividad de su correspondiente aplicación práctica, dado que los antecedentes que obran sobre este asunto no hablan, precisamente, de resultados favorables respecto de la tutela de los derechos fundamentales vinculados a la protección de los datos personales, tal y como se ha puesto de manifiesto en los párrafos expresados *ut supra*.

A este respecto, cabe reconocer que el nuevo marco normativo ha comportado un avance, en detrimento de lo que se venía efectuando hasta el momento, pero que carece aún de aquellos

[68] La Comisión Federal de Comercio de los Estados Unidos (FTC, por sus siglas en inglés), puede definirse, tal y como se efectúa a través de su propio sitio web oficial, como una agencia independiente del Gobierno estadounidense, centrada en la prevención de las prácticas comerciales anticompetitivas, engañosas o desleales hacia los consumidores, en mejorar el nivel de información de las opciones disponibles para los consumidores y aumentar el grado de comprensión del proceso competitivo por parte del público, y en cumplir con estos objetivos sin imponer una carga indebida sobre la actividad comercial legítima. Para mayor información, se ruega consultar el siguiente enlace: https://www.ftc.gov/about-ftc [consultado el 24.08.2017].

elementos indispensables que equiparen su protección a la que realiza la legislación comunitaria, teniendo en cuenta que partimos de ordenamientos jurídicos antagónicamente diferentes. Es por ello por lo que, a grandes rasgos, podríamos reconocer su positividad, debido a que ha puesto fin a la situación de inseguridad jurídica que se venía sucediendo hasta su entrada en vigor y que perjudicaba tanto a las organizaciones como a los propios particulares, pero recordando, en todo momento, que se ha seguido el mismo modelo que el adoptado para el anterior Acuerdo, introduciendo, como otra de las novedades importantes, la figura del Defensor del Pueblo como otro de los recursos a disposición de los ciudadanos europeos afectados por la recogida de sus datos personales, el cual también ha sido objeto de comentario por parte del GT29, manifestando al respecto que, aunque puede constituir una medida significante de mejora para la tutela de los derechos de los interesados, existe una preocupación por el hecho de que el órgano goce de la suficiente independencia y no ostente las suficientes competencias que le permitan desarrollar las funciones que tiene encomendadas de manera efectiva.

En definitiva, se trata de un marco normativo que viene a intentar paliar las deficiencias detectadas durante la vigencia del Acuerdo de Puerto Seguro que, finalmente, fueron manifestadas a través de la sentencia Schrems por parte del Tribunal de Justicia de la Unión Europea.

4. CONCLUSIONES

Sobre la base del análisis efectuado en las anteriores líneas, resulta oportuno señalar aquellas conclusiones que han sido alcanzadas como fruto del trabajo realizado. Es por ello por lo que, en primer lugar, a lo largo del primer apartado, se ha intentado esbozar la transición regulatoria que ha supuesto la adopción del nuevo RGPD para las transferencias internacionales, así como aquellas novedades que introduce respecto de su legislación predecesora la Directiva 95/46/CE y las posibles implicaciones que supondrá para la legislación interna de los Estados miembros, concretamente, por lo que se refiere al ámbito español. Poniéndose de manifiesto que, a grandes rasgos, aun cuando han existido novedades significativas, la estructura esencial de la que parten en su adopción no difiere en demasía de la que ya venía aplicándose en la actualidad.

En segundo lugar, podemos señalar, como se ha hecho plausible, que los esfuerzos efectuados por la Unión Europea en intentar salvaguardar y ponderar los intereses que se ponen en jaque cuando pretendemos articular una regulación para las transferencias internacionales de datos personales han resultado en vano. Esto es, por un lado, encontramos los beneficios que se obtienen de la explotación de movimientos de datos transfronterizos para los distintos operadores económicos implicados y, por otro lado, los perjuicios que esas actividades de tratamiento suponen para los derechos y libertades de las personas físicas en relación a la protección de su ámbito de privacidad e intimidad.

En tercer lugar, y en relación con lo apuntado con anterioridad, se ha procedido a analizar aquellas actuaciones efectuadas por la Unión Europea orientadas a articular un mecanismo que intentara conseguir el equilibrio apuntado. Para ello, inicialmente, pese a la condición de Estados Unidos como un país que no ofrece un nivel de protección adecuado, la Comisión Europea emitió, en fecha 26 de julio de 2000, una Decisión que pretendía articular un mecanismo que permitiera

tutelar los diferentes intereses que se hallaban en juego, objetivo que no fue alcanzado, dado que tras sendos años de vigencia y sin resultar válidamente efectiva su aplicación, el TJUE, en su sentencia de 6 de octubre de 2015, anuló la referida Decisión por no ajustarse a la protección que dimanaba, entre otros, de las vicisitudes contenidas en el artículo 25.6 de la Directiva 95/46/CE. Posteriormente, ante la inseguridad jurídica generada por la anulación adoptada por el TJUE, y si además le añadimos la constatación de que, entre otros aspectos, las autoridades norteamericanas no efectuaron un control efectivo sobre las entidades que se adherían al marco regulatorio del puerto seguro hasta que no recibieron efectivamente peticiones formales por parte de la Comisión, se propició la creación de un escenario difícil de sufragar que posibilitó la aparición, a mediados de 2016, del marco normativo sobre el escudo de privacidad que, lejos de solventar las deficiencias existentes, únicamente proponía ciertas mejoras en confrontación con las actuaciones legislativas que se habían venido sucediendo hasta la fecha, pero que difería en demasía del nivel de protección que debe resultar de aplicación a esta tipología de actividades de tratamiento de datos de carácter personal.

En cuarto lugar, cabe remarcar que tanto la Decisión de la Comisión, de 26 de julio de 2000 (Puerto Seguro) como la Decisión de ejecución (UE) n.º 2016/1250, de la Comisión, de fecha 12 de julio de 2016 (Escudo de Privacidad), no declaran que el ordenamiento jurídico norteamericano ofrezca las suficientes garantías para la protección de los datos personales, sino que además, en cierta medida, prevén, en determinados supuestos, la primacía del espectro regulatorio estadounidense frente a las estipulaciones vertidas por la legislación comunitaria. Además, cabe traer a colación que un amplio espectro de las organizaciones empresariales que estaban adheridas a los marcos regulatorios mencionados se vieron implicadas en los distintos programas de vigilancia masiva realizados por parte de las agencias de inteligencia de los Estados Unidos, hecho puesto de manifiesto a través de las revelaciones desencadenadas por parte de E. Snowden (*vid. ut supra*).

Por todo lo anterior, aunque las autoridades europeas y norteamericanas se empeñen en manifestar un consenso en el cumplimiento de la protección de los datos personales de los ciudadanos europeos a través del *EU-US Privacy Shield*[69], se hace totalmente evidente que nos encontramos ante un marco regulatorio insuficiente, que no da cumplimiento a las exigencias de protección contenidas en la normativa comunitaria, y si, a mayor abundamiento, le añadimos que la High Irish Court ha decidido remitir una cuestión prejudicial al TJUE sobre la validez de las cláusulas contractuales tipo adoptadas por las Decisiones de la Comisión Europea 2001/497/CE, 2004/915/CE y 2010/87/UE en el seno del caso Schrems, se crea un escenario para los próximos meses al que deberemos de estar expectantes, dado que se sucederán diversos cambios que podrían llegar a plantear un futuro divergente por lo que se refiere al paradigma de la protección de los datos de carácter personal.

[69] Nota de prensa conjunta, efectuada por el Departamento de Comercio de los Estados Unidos y por la Comisión Europea, en fecha 21 de septiembre 2017, sobre la revisión del Acuerdo sobre el Escudo de Privacidad UE-EE. UU. En línea: http://europa.eu/rapid/press-release_STATEMENT-17-3342_en.htm [consultado el 21.09.2017].

BIBLIOGRAFÍA

ALLEN, Anita (1988). *Uneasy Access: Privacy for Women in a Free Society*. Librería del Congreso de los EE. UU., Nueva Jersey.

ARENAS RAMIRO, Mónica (2006). *El derecho fundamental a la protección de datos personales en Europa*. Tirant lo Blanch, Valencia.

AUSLOOS, Jef. (2012). "The right to be forgotten - Worth Remembering". *Computer Law & Security Review*. Vol. 28, núm. 2, pp. 143-152.

AZURMENDI ADARRAGA, Ana (2012). "De la verdad informativa a la 'información veraz' de la Constitución Española de 1978. Una reflexión sobre la verdad exigible desde el derecho". *Comunicación y Sociedad*, núm. 18 (2), pp. 9-48.

BAÑO LEÓN, José María (2013). "La distinción entre derecho fundamental y la garantía institucional en la constitución española". Disponible *online* a 9.6.2013.

BARNES, Robin (2010). *Outrageous Invasions: Celebrities' Private Lives, Media, and the Law*. Oxford University Press.

BARRON, James (1979). "Warren & Brandeis, The Right to Privacy: Demystifying a Landmark Citation". *13 Suffolk U. L. Rev.* 875, pp. 903-907.

BENN, Stanley Isaac (1971). "Privacy, Freedom, and Respect for Persons", en Robert PENNOCK y John W. CHAPMAN (Eds.). *Nomos XII: Privacy 1, 10*. Atherton Press, Nueva York, pp. 1-26.

CABEZUELO ARENAS, Ana Laura (1998). *Derecho a la intimidad*. Tirant lo Blanch, Valencia.

MCINTYRE COOLEY, Thomas (1888). *A treatise on the law of torts or the wrongs which arise independent of contract*. 2ª ed. Callaghan and company, Chicago.

CHEMERINSKY, Erwin (2001). *Derecho Constitucional*. Aspen Law & Business, Irvine, California.

DE CUPIS, Adriano (1982). "Il diritto della personalitá", en Antonio CICU y Francesco MESSINEO (Dirs.). *Trattato di Diritto Civile e Commerciale*, Vol. 4, A. Guiffrè, Milán.

DE MIGUEL ASENSIO, Pedro (2013). *La cuestión prejudicial de la Audiencia Nacional sobre Google y la evolución de la legislación sobre protección de datos*. Blog consultado a fecha de 3 de marzo de 2012.

FRIED, Charles (1968). "Privacy". *Yale Law Journal*, vol. 77, núm. 3, pp. 475-482.

GAVISON, Ruth (1980). "Privacy and the Limits of Law". *89 Yale Law Journal*, vol. 89, núm. 3, pp. 421-440.

GUERRERO PICÓ, María del Carmen (2006). *El impacto de Internet en el Derecho fundamental a la protección de datos de carácter personal*. Civitas, Pamplona.

HEREDERO HIGUERAS, Manuel (1998). *La Directiva Comunitaria de protección de los datos de carácter personal*. Tecnos, Madrid.

HERRÁN ORTIZ, Ana Isabel (2002). *El derecho a la intimidad en la nueva ley orgánica de protección de datos*. Dykinson, Madrid.

KOOPS, Bert-Jaap (2011). "Forgetting Footprints, Shunning Shadows: A Critical Analysis of the 'Right to Be Forgotten' in Big Data Practice". *Scripted*, vol. 8, núm. 3, pp. 231-256.

MARTÍNEZ DE PISÓN CAVERO, José María (1993). *El derecho a la intimidad en la jurisprudencia constitucional*. Civitas, Madrid.

MAYER-SCHÖNBERGER, Viktor (2009). *Delete. The virtue of forgetting in the digital age*. Princeton University Press, Nueva Jersey.

MCCARTHY, J. Thomas (2013). *The rights of publicity and privacy*, 2ª ed. Clark Boardman Callaghan, California.

O'CALLAGHAN, Xavier (1991). *Libertad de expresión y sus límites: honor, intimidad e imagen*. Editorial Revista de Derecho Privado - Editorial de Derechos Reunidas, EDERSA, Barcelona.

PARKER, Richard B. "A Definition of Privacy". *Rutgers Law Review*, 27 (1974): 281.

PROSSER, William L. (1960). "Privacy". *California Law Review*, vol. 48.

RALLO LOMBARTE, Artemi (2010). "El derecho al olvido y su protección". *Revista TELOS*, núm. 85, pp. 104-108.

SALVADOR CODERCH, Pablo, *et al*. (1987). *¿Qué es difamar? Libelo contra la Ley del Libelo*. Civitas, Madrid.

SÁNCHEZ ABRIL, Patricia y LEVIN, Avner (2009). "Dos Nociones sobre la Privacidad Online". *Vanderbilt Journal of Entertainment & Technology Law*, vol. 11, pp. 1001-1051.

SIMÓN CASTELLANO, Pere (2012). *El régimen constitucional del derecho al olvido digital*. Tirant lo Blanch, Valencia.

SOLOVE, Daniel J. (2002). "Conceptualizing Privacy". *California Law Review*, vol. 90, pp. 1087 y ss.

SUÁREZ CROTHERS, Christian (2012). "El concepto de derecho a la vida privada en el derecho anglosajón y europeo". *Revista de Derecho* (Valdivia), vol. 11, pp. 103-120.

SUÑÉ LLINÁS, Emilio (2012). "La protección de datos personales en internet". *II Congreso Mundial de Derecho Informático*. Disponible *online* a fecha de 28.3.2012.

TÉLLEZ AGUILERA, Abel (2002). *La protección de datos en la Unión Europea. Divergencias normativas y anhelos unificadores*. Edisofer, Madrid.

TRONCOSO REIGADA, Antonio (2012). "Hacia un nuevo marco jurídico europeo de protección de datos personales". *Revista Española de Derecho Europeo*, núm. 43, pp. 25-160.

— (2013). "El derecho al olvido en Internet a la luz de la propuesta de Reglamento General de Protección de Datos Personales". Disponible *online* a fecha de 14.4.2013.

VOLOKH, Eugene (2000). "Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You". *Stanford Law Review* 52, pp. 1049.

WARREN, Samuel y BRANDEIS, Louis (1890). "The Right to Privacy". *Harvard Law Review*, vol. IV, núm. 15, pp. 2303-2312.

www.icps.cat