TRABAJO DE FINAL DE GRADO

LAS TRANSFERENCIAS INTERNACIONALES DE DATOS PERSONALES A ESTADOS UNIDOS DE AMÉRICA Y LA INVALIDEZ DEL RÉGIMEN DEL *SAFE HARBOUR*

Autora:

Raquel GÓMEZ MUÑOZ

Director del Trabajo:

Josep CAÑABATE PÉREZ

Trabajo de Final de Grado

Cuarto curso del Grado en Derecho

Facultad de Derecho

Departamento de Ciencia Política y Derecho Público

En Bellaterra, a 13 de mayo de 2016

ÍNDICE

RESUMEN 7

ABREVIATURAS 8

INTRODUCCIÓN 10

I. JUSTIFICACIÓN DE LA ELECCIÓN DEL OBJETO DE ESTUDIO 10

II. OBJETIVOS GENERALES Y ESPECÍFICOS 13

III. METODOLOGÍA DE INVESTIGACIÓN 14

CAPÍTULO I. LA EVOLUCIÓN DEL DERECHO A LA PROTECCIÓN DE LOS DATOS PERSONALES HASTA SU CONSAGRACIÓN COMO DERECHO FUNDAMENTAL AUTÓNOMO 16

CAPÍTULO II. LA REGULACIÓN DEL DERECHO A LA PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL. 18

I. NORMATIVA EUROPEA Y COMUNITARIA. 18

II. NORMATIVA ESTATAL. 20

CAPÍTULO III. LA INSTITUCIÓN JURÍDICA DE LA "TRANSFERENCIA INTERNACIONAL DE DATOS". 21

I. EL CONCEPTO DE "TRANSFERENCIA INTERNACIONAL DE DATOS". 21

II. EL REQUISITO ESENCIAL DE VALIDEZ DE LA TRANSFERENCIA INTERNACIONAL DE DATOS: CUMPLIMIENTO DE LA LOPD Y DEL REGLAMENTO DE LA LOPD. 26

1. Creación de un fichero de titularidad privada. 27

2. El régimen de la cesión o comunicación de datos. 28

III. ÁMBITO SUBJETIVO DE LA TRANSFERENCIA INTERNACIONAL DE DATOS. 31

IV. ÁMBITO OBJETIVO DE LA TRANSFERENCIA INTERNACIONAL DE DATOS. 34

1. Las transferencias a terceros Estados que garantizan un "nivel de protección adecuado": la norma general. 34

2. Las transferencias a terceros Estados que no garantizan un "nivel de protección adecuado". 37

2.1. Excepciones a la norma general previstas por la Directiva 95/46/CE y la LOPD. 37

2.2. La presentación de "garantías suficientes" por el responsable del tratamiento de datos de carácter personal. 39

2.2.1. Cláusulas contractuales tipo 40

2.2.2. Normas corporativas vinculantes ("*Binding Corporate Rules*" o "BCR") 42

CAPÍTULO IV. LAS TRANSFERENCIAS INTERNACIONALES DE DATOS EN EL REGLAMENTO (UE) 2016/679 DEL PARLAMENTO Y DEL CONSEJO, DE 27 DE ABRIL DE 2016. 43

CAPÍTULO V. LAS TRANSFERENCIAS INTERNACIONALES DE DATOS CON DESTINO A ESTADOS UNIDOS DE AMÉRICA. 47

I. LA PROTECCIÓN JURÍDICA DE LOS DATOS PERSONALES EN ESTADOS UNIDOS DE AMÉRICA. 47

1. Instrumentos normativos que protegen los datos personales en Estados Unidos de América. 47

2. Evolución de los mecanismos de protección de los datos personales en Estados Unidos de América. 50

II. ANÁLISIS CRÍTICO DE LA DECISIÓN DE LA COMISIÓN EUROPEA DE 26 DE JULIO DE 2000 SOBRE LA ADECUACIÓN CONFERIDA POR LOS PRINCIPIOS DE PUERTO SEGURO PARA LA PROTECCIÓN DE LA VIDA PRIVADA Y LAS CORRESPONDIENTES PREGUNTAS MÁS FRECUENTES. 53

1. Elementos de carácter formal 55

1.1. La inadecuación del artículo 1 de la Decisión al del artículo 25.6 de la Directiva 95/46/CE. 55

1.2. El sistema de adhesión a los Principios de Puerto Seguro y sus límites. 56

2. Elementos de carácter material 58

2.1. La ambigüedad del ámbito de aplicación de la Decisión de la Comisión de 26 de julio de 2000 y las competencias limitadas de los organismos públicos enumerados en el anexo VII de la Decisión. 58

2.2. La ineficacia del sistema de verificación que prevé la Pregunta más Frecuente número 7. 61

2.3. Los límites al ejercicio de los derechos de opción y de acceso en la Decisión de la Comisión de 26 de julio de 2000 y la formulación del principio de notificación. 63

2.4. La pérdida del control de los datos personales en las transferencias ulteriores. 67

2.5. El papel de las autoridades nacionales de supervisión de los Estados miembros de la UE. 69

III. PROBLEMAS EN LA APLICACIÓN DE LOS PRINCIPIOS DE PUERTO SEGURO Y DE LAS PREGUNTAS MÁS FRECUENTES. 70

1. Un nuevo contexto de desarrollo de la economía digital. 70

2. La falta de transparencia y de control en la ejecución del régimen de 71

puerto seguro y su incumplimiento por las empresas autocertificadas.

3. La vigilancia de las comunicaciones electrónicas a los efectos de inteligencia y seguridad nacional en Estados Unidos de América. 73

IV. LA SENTENCIA DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, DE 6 DE OCTUBRE DE 2015. 78

1. Antecedentes de hecho de la Sentencia del Tribunal de Justicia de la Unión Europea, de 6 de octubre de 2015. 78

2. Sobre la validez de la Decisión 2000/520. 79

3. Consecuencias de la Sentencia del TJUE de 6 de octubre de 2015. 82

V. EL NUEVO ACUERDO *EU-US PRIVACY SHIELD* 84

VI. ANÁLISIS DE LA POLÍTICA DE DATOS DE FACEBOOK. 85

CONLUSIONES 89

BIBLIOGRAFÍA 94

ANEXO 103

RESUMEN

A lo largo del presente trabajo se analiza en profundidad el concepto y la regulación de la institución de la transferencia internacional de datos personales, tanto a nivel europeo como español y, en particular, se examina el marco jurídico que, desde el año 2000, ha canalizado las transferencias que se han venido realizando desde la Unión Europea a Estados Unidos de América: la Decisión de la Comisión Europea de 26 de julio de 2000 sobre la adecuación conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes. El mencionado estudio se efectúa atendiendo a los documentos emitidos por el Grupo de Trabajo del Artículo 29 y por la Comisión, así como a las razones que han llevado al Tribunal de Justicia de la Unión Europea a declarar la invalidez de la Decisión en su Sentencia de 6 de octubre de 2015.

Además, se examinan ciertos sucesos que han tenido lugar desde la publicación de la Sentencia del Tribunal de Justicia de la Unión Europea, como la celebración del acuerdo EU-US Privacy Shield, la aprobación del nuevo Reglamento general de protección de datos a nivel de la Unión Europea, así como el contenido de las Políticas de datos de Facebook tras la anulación del régimen de Puerto Seguro o *Safe Harbour*.

ABREVIATURAS

CE: Constitución Española de 1978

LOPD: Ley Orgánica 15/1999, de 14 de diciembre, de Protección de Datos de Carácter Personal

LO 1/1982: Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la propia imagen

Directiva 95/46/CE: Directiva 95/46/CE, del Parlamento 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

Reglamento general de protección de datos: Reglamento (UE) 2016/679 del Parlamento 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

Reglamento de la LOPD: 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.

TFUE: Tratado de Funcionamiento de la Unión Europea

UE: Unión Europea

TJUE: Tribunal de Justicia de la Unión Europea

Comisión: Comisión Europea

EE.UU: Estados Unidos de América

TC: Tribunal Constitucional

AEPD: Agencia Española de Protección de Datos GT29: Grupo de Trabajo del Artículo 29

Decisión: Decisión nº 520 de la Comisión Europea de 26 de julio de 2000 sobre la adecuación conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes.

FAQ: Frequently Asked Questions

USA PATRIOT Act: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act

FBI: Federal Bureau of Investigation

FISC: Foreign Intelligence Surveillance Court

FISA: Foreign Intelligence Surveillance Act

TJUE: Tribunal de Justicia de la Unión Europea

NSA: National Security Agency

ADR: Alternative Dispute Resolution

INTRODUCCIÓN

I. JUSTIFICACIÓN DE LA ELECCIÓN DEL OBJETO DE ESTUDIO

El presente Trabajo de Final de Grado pretende efectuar un análisis exhaustivo de la institución de la transferencia internacional de datos personales, como mecanismo jurídico que canaliza el fenómeno de la globalización de los datos personales y que, en ocasiones, comporta la ineficacia de la normativa europea en el campo de la protección de los datos personales.

En lo que a los medios de protección de los datos se refiere, si bien se ha producido un efecto homogeneizador respecto del movimiento de datos personales entre los países miembros de la Unión Europea (en adelante, "UE") –proceso que ha culminado con la aprobación del Reglamento General de Protección de Datos por el Parlamento Europeo el 14 de abril de 2016- por razones económicas dichos países deben afrontar el movimiento internacional de datos hacia terceros países. Y ello porque la información, como señala JAN HOLVAST[1], tiene dos importantes características: "*it is power and it is money"*.

El objeto de estudio se circunscribe al análisis de la regulación europea y española respecto las transferencias internacionales de datos a terceros Estados no miembros de la Unión Europea y, en concreto, de las transferencias que se realizan a Estados Unidos de América (en adelante, "EE.UU"), calificado como primer país importador de datos transferidos desde España[2]. Así pues, se prohibirá con carácter general toda transferencia transatlántica de datos personales a EE.UU cuando no se garantice un "nivel de protección adecuado" de los derechos fundamentales de sus titulares.

Los argumentos que justifican la elección del mencionado objeto de estudio se hallan estrechamente conectados con el entorno social y económico que encierra toda trasferencia internacional de datos personales. Por una parte, como señala ORTEGA GIMÉNEZ, "el perfeccionamiento de las tecnologías de la información y de la

[1] Vid. HOLVAST, Jan, "History of Privacy", en DE LEEUW, Karl y BERGSTRA, Jan (eds.) *The History of Information Security: A Comprehensive Handbook*, Ed. Elsevier, Ámsterdam, 2007, p. 14.
[2] Vid. ORTEGA GIMÉNEZ, Alfonso, *La (des)protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita*, Agencia Española de Protección de datos, Alicante, 2014, p. 21.

comunicación ha favorecido el flujo global y exponencial de información"[3], por ello, en la actualidad, el régimen previsto para las transferencias internacionales de datos y su efectividad en relación con la protección de los derechos fundamentales de los sujetos afectados va ocupando cada vez más importancia.

Por otra parte, y debido al contexto social y cultural que envuelve a la sociedad de la primera década del siglo XXI, la cesión "consentida" de datos por parte de sus titulares a empresas –que, en muchas ocasiones son estadounidenses-, ha devenido una práctica diaria. Según el informe de OBS[4], España cuenta con una población online de 23 millones de personas, el 73% de la cual ha utilizado activamente las redes sociales en 2014, y únicamente el 8% dice no tener cuenta en ninguna red.

Dicho lo anterior, hoy en día la presión social fomenta la cesión continua de datos personales, hallándose cada vez más reducido el contenido del "derecho a la intimidad", definido por el Tribunal Constitucional en 1997[5] como ese "ámbito más reservado de las personas que desea mantenerse oculto a los demás por pertenecer a su esfera más privada". Más no se trata tan sólo de cuestionar la conveniencia de dichas prácticas, cuanto que existe una confianza que en realidad es infundada en las compañías estadounidenses que tratan los datos personales de sus usuarios.

A lo largo del presente trabajo se constatará que, pese a la semejante concepción del contenido del derecho a la privacidad o *privacy* en Europa y EE.UU, su protección y alcance serán muy distintos[6]. Así las cosas, desde la entrada en vigor de la Directiva 95/46/CE, de 24 de octubre de 1995, las relaciones entre los EE.UU y la Unión Europea no han sido del todo pacíficas, tal es así que algunos autores han llegado a calificarlas de "*Privacy Trade War"*[7].

Siendo patente la necesidad de asegurar el libre flujo de información entre la Unión Europea y EE.UU., y tras años de negociaciones entre la Comisión Europea y el *US Department of Commerce*, se confeccionó el sistema de Principios de Puerto Seguro o

[3] Vid. ORTEGA GIMÉNEZ, *La (des)protección del titular*, ob. cit., p. 18.
[4] Vid. Online Business School presenta el estudio **Social Media 2015**, que analiza las tendencias de uso y participación en redes sociales tanto en España como en las principales economías mundiales, en línea: http://www.obs-edu.com/noticias/estudio-obs/espana-aumenta-el-numero-de-usuarios-activos-en-redes-sociales-en-2014-y-llega-los-17-millones/ [consultado el 10.12.2015].
[5] Vid. Sentencia del Tribunal Constitucional 151/1997, de 29 de septiembre.
[6] Vid. ARRIBAS LUQUE, José María, "Sobre la protección adecuada en las transmisiones de datos personales desde la Unión Europea a los EE.UU.: El sistema de principios de Puerto Seguro", *Diario La Ley*, nº 549 (2002), p. 2.
[7] Vid. ARRIBAS LUQUE, ob. cit., p. 6.

Safe Harbor Privacy Principles, interpretado y desarrollado por las *Frecuently Asked Questions*, también denominadas "*FAQ*", todo ello publicado el 21 de julio del 2000 por el *US Department of Commerce.* En virtud de la potestad otorgada a la Comisión Europea mediante el artículo 25.6 de la Directiva 95/46/CE, conforme a la cual puede hacer constar que un país tercero garantiza un nivel de protección adecuado, ésta declaró que el sistema de Principios de Puerto Seguro estadounidense se ajustaba a la normativa europea de protección de datos, al asegurar un adecuado nivel de protección en las transferencias internacionales de datos personales a EE.UU, y ello lo llevó a cabo mediante su Decisión 2000/520/CE, de 26 de julio (en adelante, "Decisión").

Asimismo, para la preparación de la mencionada Decisión la Comisión tuvo en cuenta los dictámenes emitidos por el Grupo de trabajo de protección de las personas, también denominado "Grupo del artículo 29", que ha venido publicando orientaciones sobre el nivel de protección de los datos que proporcionan los principios en los EE.UU. En síntesis, y de acuerdo con el Considerando quinto y séptimo de la Decisión, el nivel adecuado de protección de la transferencia de datos desde la UE a EE.UU debe alcanzarse si el Departamento de Comercio de los EE.UU o su representante se compromete a mantener y poner a disposición del público una lista de las entidades que autocertifiquen su adhesión a los principios y su aplicación conforme a las FAQ, debiendo dichas entidades dar a conocer públicamente sus políticas de protección de la vida privada y someterse a la jurisdicción de la *Federal Trade Commission* (en adelante, "FTC") en virtud de lo dispuesto en el artículo 5 de la *Federal Trade Commission Act*.

Tras la revelación por el periódico británico *The Guardian,* el 5 de junio de 2013, de las actividades de vigilancia masivas e indiscriminadas llevadas a cabo por los servicios de inteligencia de Estados Unidos a millones de ciudadanos, basándose en la documentación suministrada por Edward Snowden, antiguo trabajador de la *National Security Agency* (en adelante "NSA"), se inició un debate internacional acerca la eficacia del régimen de Puerto Seguro.

Finalmente, la Sentencia del Tribunal de Justicia de la Unión Europea, de 6 de octubre de 2015, anuló la Decisión 2000/520/CE de la Comisión considerando que los principios de Puerto Seguro y las FAQ realmente no garantizaban un nivel adecuado de protección de los datos personales transferidos desde la UE a las entidades norteamericanas adheridas a los mismos.

Como se ha apuntado con anterioridad, a ello debe añadirse la aprobación por el Parlamento Europeo, el 14 de abril de 2016, del nuevo Reglamento General de Protección de Datos mediante el cual se ha derogado la Directiva 95/46/CE, que puso fin a más de cuatro años de trabajo para reformar de forma contundente la normativa comunitaria sobre protección de datos. En efecto, las reglas de la antigua Directiva se crearon cuando el uso de internet no estaba tan extendido, por ello, la nueva normativa pretende aumentar el control de los datos personales de los ciudadanos en un mundo de teléfonos inteligentes, redes sociales, banca por internet y transferencias globales.

II. OBJETIVO GENERAL Y OBJETIVOS ESPECÍFICOS.

La finalidad principal de este trabajo es, tras examinar la regulación de las transferencias internacionales de datos tanto en el ordenamiento jurídico comunitario como en el español, analizar y reflexionar sobre el régimen previsto para las transferencias internacionales de datos que se realizan desde la Unión Europea a Estados Unidos de América, en particular, el régimen de Puerto Seguro o *Safe Harbour* previsto en la Decisión de la Comisión de 26 de julio de 2000, declarado inválido por la Sentencia del Tribunal de Justicia de la Unión Europea, de 6 de octubre de 2015.

En segunda instancia, me propongo satisfacer cuatro objetivos más específicos que se hallan estrechamente conectados con la pretensión principal del trabajo. En primer lugar, si bien el trabajo tendrá como normativa de referencia la prevista en la Directiva 95/46/CE, 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, así como la contenida en su instrumento de transposición al ordenamiento jurídico español, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, dado que el día 14 de abril de 2016 el Parlamento Europeo aprobó el Reglamento general de protección de datos, tras haber manifestado su posición favorable el Consejo Europeo el pasado 8 de abril, se dedicará el Capítulo IV al estudio de las novedades introducidas por el mismo con respecto al régimen de las transferencias internacionales de datos.

En segundo lugar, me propongo conocer el sistema de protección jurídica de los datos personales en Estados Unidos de América y, de este modo, comprender tanto los

problemas que han existido en relación con la aplicación del régimen del *Safe Harbour* como los motivos que esgrimió el Tribunal de Justicia de la Unión Europea para declarar la invalidez de la Decisión de la Comisión de 26 de julio de 2000.

En tercer lugar, pretendo exponer de forma sintética las novedades que se pretenden incluir en el nuevo acuerdo EU-US *Privacy Shield* en relación a lo que ya preveía el acuerdo del *Safe Harbour*.

Por último, dado que Facebook es una de las redes más usadas por los internautas españoles[8], me propongo examinar el contenido de la "Política de datos" de esta red social, así como las "Condiciones" de dicho servicio, también denominadas "Declaración de derechos y responsabilidades".

III. METODOLOGÍA DE INVESTIGACIÓN

Concretado el objeto de estudio y explicadas las razones que justifican su elección, a continuación se procederá a exponer la metodología que se seguirá a lo largo de la investigación a los efectos de satisfacer la pretensión principal y los objetivos específicos del presente estudio.

Después de exponer la constitucionalización del derecho a la protección de los datos personales en el Capítulo I, el estudio prosigue con un análisis exhaustivo de los mecanismos de protección de los datos personales existentes en Europa y España, en el Capítulo II.

A continuación, en el Capítulo III, tras delimitar el concepto de "transferencia internacional de datos" y exponer sus requisitos, se analiza el ámbito subjetivo y objetivo de esta institución, constatando los derechos que tienen los titulares de los datos personales en el marco de las transferencias internacionales de datos. Para la verificación de tal estado de las cosas se examinarán, en primer lugar, las distintas categorías de producción normativa, empezando por la regulación contenida en la Directiva 95/46/CE, de 24 de octubre de 1995, continuando por su instrumento de

[8] Vid. Online Business School presenta el estudio **Social Media 2015**, que analiza las tendencias de uso y participación en redes sociales tanto en España como en las principales economías mundiales, en línea: http://www.obs-edu.com/noticias/estudio-obs/espana-aumenta-el-numero-de-usuarios-activos-en-redes-sociales-en-2014-y-llega-los-17-millones/ [consultado el 10.12.2015].

transposición al ordenamiento jurídico español, la LO 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, así como su Reglamento de desarrollo el Real Decreto 1720/2007, de 21 de diciembre. También se atenderá a la Jurisprudencia del Tribunal de Justicia de la Unión Europea, a los documentos de la Comisión y del Grupo de Trabajo del artículo 29, así como a la doctrina de autores especializados en esta materia.

Dada la reciente aprobación del Reglamento general de protección de datos en el ámbito de la Unión Europea, se dedicará el Capítulo IV del presente estudio a las novedades introducidas por el mismo con respecto al régimen de las transferencias internacionales de datos.

En el Capítulo V, tras exponer de forma simplificada la protección jurídica que se otorga en Estados Unidos a los datos de carácter personal, se efectúa un análisis crítico de la Decisión de la Comisión de 26 de Julio de 2000, que versa sobre la adecuación conferida por los Principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes. Deseo subrayar que para la confección de dicho análisis se atenderá especialmente a los documentos emitidos por la Comisión Europea y por el Grupo de Trabajo del Artículo 29.

A continuación, se examinarán los problemas que se han venido suscitando en relación con la aplicación de la Decisión de la Comisión de 26 de julio de 2000 y ello para la mejor comprensión de las razones que han llevado al Tribunal de Justicia de la Unión Europea a su anulación mediante su Sentencia de 6 de octubre de 2015. Por último, se detallarán las novedades que se pretenden incluir en el nuevo acuerdo EU-US *Privacy Shield* en relación a lo que ya preveía el acuerdo del *Safe Harbour* y se examinará el contenido de la "Política de datos" y de las "Condiciones" de la red social Facebook.

CAPÍTULO I

LA EVOLUCIÓN DEL DERECHO A LA PROTECCIÓN DE LOS DATOS PERSONALES HASTA SU CONSAGRACIÓN COMO DERECHO FUNDAMENTAL AUTÓNOMO

En España el derecho a la intimidad viene recogido en el artículo 18 de la Constitución de 1978 (en adelante, "CE" o "Constitución") que, junto a la declaración general de positivización del derecho, y tras recoger sus distintas manifestaciones, finaliza con la proclamación del *habeas data*[9] o faceta informática de la intimidad[10].

No obstante, cabe señalar que la Constitución no contempla la protección de datos de carácter personal como derecho fundamental, aunque su artículo 18.4, junto a los artículos 10.1[11] y 18.1, serán el punto de apoyo para su posterior consideración como derecho fundamental por la jurisprudencia constitucional[12].

La Sentencia del Tribunal Constitucional núm. 254/1993, de 20 de julio[13] menciona por primera vez la denominada "libertad informática", como derecho o libertad que debe garantizarse a todo ciudadano, cuyo contenido más "elemental" era negativo, apuntando que *"el uso de la informática encuentra un límite en el respeto al*

[9] "Nuestra norma suprema establece que la ley ha de limitar el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos, como una garantía de inviolabilidad (…) frente a la posibilidad de que el Estado pudiera entrometerse en sus vidas privadas y en su derecho a la intimidad. Sin embargo, con el paso de los años y el desarrollo tecnológico, este enfoque ha variado y se ha centrado más en la privacidad como manifestación del derecho a la intimidad". CÁRDENAS ARTOLA, Ignacio; FERRERO RECASENS, Eduardo, entre otros, *Memento experto. Protección de datos,* Ed. Francis Lefebvre, Madrid, 2012, p. 15.

[10] Vid. BRU CUADRADA, Elisenda, "La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad", *Revista de Estudios de Derecho y Ciencia Política de la UOC*, nº 5, (2007), p. 83.

[11] Artículo 10.1 de la Constitución Española: "*La dignidad de la persona, los derechos inviolables que le son inherentes, el libre desarrollo de la personalidad, el respeto a la ley y a los derechos de los demás son fundamento del orden político y de la paz social*".

[12] Vid. REBOLLO DELGADO, Lucrecio, *Manual de protección de datos,* Ed. Dykinson, Madrid, 2014, p. 61.

[13] De acuerdo con el Tribunal Constitucional, "*esta constatación elemental de que los datos personales que almacena la Administración son utilizados por sus autoridades y sus servicios impide aceptar la tesis de que el derecho fundamental a la intimidad agota su contenido en facultades puramente negativas, de exclusión. Las facultades precisas para conocer la existencia, los fines y los responsables de los ficheros automatizados dependientes de una Administración pública donde obran datos personales de un ciudadano son absolutamente necesarias para que los intereses protegidos por el art. 18 CE, y que dan vida al derecho fundamental a la intimidad, resulten real y efectivamente protegidos. Por ende, dichas facultades de información forman parte del contenido del derecho a la intimidad, que vincula directamente a todos los poderes públicos, y ha de ser salvaguardado por este Tribunal, haya sido o no desarrollado legislativamente*". Sentencia del Tribunal Constitucional núm. 254/1993, de 20 de julio (Rec. 1827/1990).

honor y la intimidad de las personas y en el pleno ejercicio de sus derechos". No obstante, el Tribunal añade que para la efectividad de este derecho debe añadirse una "garantía complementaria", que adopta un contenido positivo pues, *"la llamada libertad informática es, así, también, el derecho a controlar el uso de los mismos datos insertos en un programa informático (habeas data)"*[14].

Siete años después, el mismo Tribunal, en respuesta a un recurso de inconstitucionalidad interpuesto por el Defensor del Pueblo contra algunos incisos de los artículos 21.1, 24.1 y 24.2 de la Ley Orgánica 15/1999, de 14 de diciembre, de Protección de Datos de Carácter Personal (en adelante, "LOPD"), fue quien consagró la protección de datos de carácter personal como un derecho fundamental autónomo y diferente del derecho a la intimidad. Ello lo llevó a cabo en su Sentencia núm. 292/2000, de 30 de noviembre, señalando que "*la función del derecho fundamental a la intimidad del art. 18 CE es la de proteger frente a cualquier invasión que pueda realizarse en aquel ámbito de la vida personal y familiar que la persona desea excluir del conocimiento ajeno y de las intromisiones de terceros en contra de su voluntad. En cambio, el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado*"[15], gozando este último de un objeto más amplio que el del derecho a la intimidad.

En esta Sentencia también se delimita la estructura y el contenido del derecho fundamental a la protección de datos de carácter personal, y ello lo hace el TC apuntando que "*el contenido del derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de estos datos proporcionará a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o no*"[16].

[14] Vid. Sentencia del Tribunal Constitucional núm. 254/1993, de 20 de julio (Rec. 1827/1990), Fundamento Jurídico Séptimo.
[15] Vid. Sentencia del Tribunal Constitucional núm. 292/2000, de 30 de noviembre (Rec. 1463/2000), Fundamento Jurídico Sexto.
[16] Vid. Sentencia núm. 292/2000, de 30 de noviembre (Rec. 1463/2000), Fundamento Jurídico Séptimo.

CAPÍTULO II

LA REGULACIÓN DEL DERECHO A LA PROTECCIÓN DE LOS DATOS DE CARÁCTER PERSONAL

I. NORMATIVA EUROPEA Y COMUNITARIA.

En 1981 se aprobó el Convenio nº 108 del Consejo de Europa de 28 de enero, sobre protección de las personas en lo relativo al tratamiento automatizado de datos de carácter personal, la primera norma europea que marcó las pautas del modelo común de protección de datos[17]. Es también significativa la Recomendación de la OCDE sobre los principios relativos a la protección de la privacidad y transferencia internacional de datos personales, adoptada el 23 de septiembre de 1980[18].

En lo que al ámbito comunitario se refiere, y sobre la base de los principios aportados por el Convenio, se confeccionó la Directiva 95/46/CE, del Parlamento 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 adelante, "Directiva 95/46/CE"). También, el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, de 7 de diciembre del 2000, como documento que reafirma los derechos reconocidos por las tradiciones constitucionales y las obligaciones internacionales comunes de los Estados miembros, reconoce explícitamente el derecho a la protección de los datos de carácter personal.

Desde la entrada en vigor de la Directiva 95/46/CE, los Estados miembros de la Unión Europea, a los efectos de cumplir con la obligación de su transposición, han ido elevando progresivamente el nivel de protección de los datos personales, produciéndose un "efecto homogeneizador de los medios de protección y de los mecanismos para la eficacia de los derechos"[19]. Como resultado de este proceso, la normativa de la Unión

[17] Vid. BRU CUADRADA, Elisenda, ob. cit., p. 82.
[18] "Los principios de la Recomendación de la OCDE pueden servir de inspiración al legislador nacional, habida cuenta del carácter no obligatorio de este instrumento". Difieren en sus desarrollos, en la mayor preocupación del Convenio de 1980 en lo que respecta a la dimensión de aseguramiento y protección de la vida privada, frente a la orientación suscrita por la OCDE más sensible a las necesidades de la circulación de los datos en el marco del desarrollo económico y social". SANCHO VILLA, Diana, *Transferencia internacional de datos personales,* Agencia de Protección de Datos, Madrid, 2003, p. 55 y 56.
[19] Vid. REBOLLO DELGADO, Lucrecio, ob. cit., p. 39.

Europea en el campo de la protección de los datos ha devenido la más exigente del planeta[20].

En síntesis, la Directiva 95/46/CE, que se halla estructurada en 7 Capítulos, tras definir su objeto, delimitar los conceptos más esenciales y establecer su ámbito de aplicación, expone las "*condiciones generales para la licitud del tratamiento de los datos personales*". En ellas se contienen los principios esenciales del derecho a la protección de los datos personales y los derechos de que gozan los interesados, cuyos datos personales son objeto de tratamiento[21]. También, la Directiva lleva a cabo un mandato de creación de una autoridad de control que vele por el cumplimiento de la normativa de protección de datos personales[22], así como de constitución de un "grupo de protección de las personas en lo que respecta al tratamiento de los datos personales", comúnmente denominado "Grupo de trabajo del artículo 29"[23].

Como consecuencia de la rápida evolución tecnológica, así como de la necesidad de dar uniformidad al régimen jurídico en materia de protección de datos entre todos los Estados Miembros, el 25 de enero de 2012 se publicó la Propuesta de Reglamento[24] del Parlamento Europeo y del Consejo 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. Finalmente, tras cuatro años de trabajo, el día 14 de abril de 2016 el Parlamento Europeo adoptó el Proyecto de Reglamento general de protección de datos, tras haber manifestado su posición favorable el Consejo Europeo el pasado 8 de abril.

---

[20] Vid. GUASCH PORTAS, Vicente, *Las transferencias internacionales de datos en la normativa española y comunitaria*, Agencia Española de Protección de Datos y Agencia Estatal Boletín Oficial del Estado, Madrid, 2014, p. 22.

[21] Hablamos de los principios relativos a la calidad de los datos –que sean tratados de manera leal y lícita, recogidos con fines determinados y no sean tratados posteriormente de manera incompatible con dichos fines, adecuados, pertinentes y no excesivos, exactos, actualizados, etcétera-; de los principios relativos a la legitimación del tratamiento de datos –que el tratamiento sólo se efectúe si el interesado haya dado su consentimiento de forma inequívoca, para el cumplimiento de una misión de interés público, que sea necesario para proteger el interés vital del interesado, etcétera-; de la especial protección de las "categorías especiales de tratamientos"; del derecho a la información del interesado; del derecho de acceso del interesado a los datos; del derecho de oposición del interesado; y del deber confidencialidad y seguridad del tratamiento, así como de notificación a la autoridad de control de aquello que se determine legalmente. Capítulo II de la Directiva 95/46/CE.

[22] Vid. Considerando 62 y artículo 28 y ss. de la Directiva 95/46/CE.

[23] El Grupo se halla compuesto por un representante de la autoridad o autoridades de control designadas por cada Estado miembro, por un representante de la autoridad/es creadas por las instituciones y organismos comunitarios y por un representante de la Comisión. Artículo 29.2 de la Directiva 95/46/CE.

[24] "La elección del instrumento del Reglamento, norma jurídica del Derecho comunitario cuyo alcance es general y su eficacia directa, hacen que la aplicabilidad de las normas en él recogidas sean obligatorias para todos los Estados Miembros, desde su entrada en vigor" CÁRDENAS ARTOLA, Ignacio; FERRERO RECASENS, Eduardo, entre otros, ob. cit., p. 19.

Con el objetivo de efectuar una reforma intensa de la normativa comunitaria sobre protección de datos, adaptándola al contexto social y tecnológico actual, así como de homogeneizar su aplicación en todos los Estados Miembros de la UE, el Reglamento (UE) 2016/679 del Parlamento 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 (en adelante, "Reglamento general de protección de datos" o "Reglamento") ha sustituido a la Directiva 95/46/CE, cuya normativa ha sido la base fundamental del presente trabajo.

II. NORMATIVA ESTATAL

El desarrollo legislativo del derecho se lleva a cabo mediante dos leyes: la Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la propia imagen (en adelante, "LO 1/982") y la Ley Orgánica 15/1999, de 13 de diciembre de 1999, de Protección de Datos de Carácter Personal.

Hasta LOPD, la protección del contenido del art. 18.4 CE se llevaba a cabo en base a la LO 1/1982[25]. Así las cosas, en 1992 se promulgó la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, que nació "*para hacer frente a los riesgos que para los derechos de la personalidad puede suponer el acopio y tratamiento de datos por medios informáticos*"[26], teniendo por objeto "*limitar el uso de la informática y otras técnicas y medios de tratamiento automatizado de los datos de carácter personal para garantizar el honor, la intimidad personal y familiar de las personas físicas y el pleno ejercicio de sus derecho*"[27].

Más adelante, y a los efectos de cumplir con la obligación comunitaria de transposición de la Directiva 95/46/CE, en diciembre de 1999 se publicó la hoy vigente LOPD, cuyo objeto y ámbito de aplicación se concreta en su artículo 1, afirmando que "*La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne*

[25] Vid. REBOLLO DELGADO, Lucrecio, ob. cit., p. 65.
[26] Vid. Exposición de Motivos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.
[27] Vid. Artículo 1 de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal.

al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familia". Así, mientras la antigua Ley tenía una formulación de carácter negativo, pretendiendo "limitar" las facultades de uso de la informática para velar por los derechos fundamentales de los ciudadanos, la LOPD opta por una formulación positiva, al tener por objeto "garantizar y proteger" los mencionados derechos.

CAPÍTULO III

LA INSTITUCIÓN JURÍDICA DE LA "TRANSFERENCIA INTERNACIONAL DE DATOS"

I. EL CONCEPTO DE "TRANSFERENCIA INTERNACIONAL DE DATOS".

El tráfico internacional de datos personales[28] se canaliza jurídicamente mediante transferencias internacionales de datos, desde el ordenamiento que los califica de ese modo –como datos personales-, a un destinatario establecido en un territorio extranjero[29]. Esta institución jurídica merece especial atención tanto desde un punto de

[28] "El crecimiento de los flujos internacionales de información ha multiplicado las solicitudes de autorización de transferencias internacionales de datos de carácter personal: comunicaciones de datos personales entre las filiales de una empresa multinacional, utilización de herramientas multiacceso, prestación de servicios desde distintos países, o la gestión integral de los procesos de recursos humanos de una multinacional, están a la orden del día. El aumento de las transferencias internacionales de datos personales en áreas tales como la de los recursos humanos, los servicios financieros, la banca, la educación, el comercio electrónico, el auxilio judicial internacional o la investigación en el área de la salud son ahora una parte integral de la economía globalizada. En materia de regulación de la protección de datos de carácter personal pueden diferenciarse tres grandes grupos. Un primer grupo formado por los Estados donde existe legislación en materia de protección de datos actual, vigente y adaptada al momento actual (p. ej., sería el caso de los Estados miembros de la UE, Argentina, México, Canadá o EE. UU.); el segundo grupo, el formado por aquellos países en los que se está trabajando en pro de una legislación en materia de protección de datos (p. ej. en algunos países de la región latinoamericana, como en Perú, Ecuador, Colombia, Chile o Uruguay) se están planteando en la actualidad «adaptaciones» de su legislación en materia de protección de datos); y el tercer grupo es el integrado por aquellos países donde, a día de hoy, la legislación en materia de protección de datos brilla por su ausencia (el caso, p. ej., de países como Rusia, Malasia o Taiwán). ORTEGA GIMÉNEZ, Alfonso, La (des)protección del titular, ob. cit., p. 20.

[29] Vid. SANCHO VILLA, Diana, *Transferencia internacional*, ob. cit., p. 25 y 26.

vista socioeconómico como jurídico pues, como señala DURÁN CARDO[30], es uno de los aspectos más importantes de la regulación contenida en la Directiva 95/46/CE[31].

De acuerdo con GUASCH PORTAS, la estructura implantada en la Unión Europea puede llevar a unos resultados satisfactorios en el mercado interior en materia de protección de datos, pero puede carecer de eficacia si no se establecen los mecanismos adecuados con respecto al movimiento internacional de datos con terceros países[32]. Así, las transferencias internacionales de datos entrañan riesgos, pues pueden suponer, por una parte, la pérdida de control de los propios datos por parte del sujeto afectado, sin que posteriormente pueda ejercer sus "derechos ARCO"[33] –de ahí la importancia de la concurrencia de su consentimiento y, por otra parte, la posibilidad de reutilización de los mismos para una finalidad distinta de la autorizada –que se pone en relación con el principio de calidad de los datos-.

Por ello, la preocupación respecto las transferencias internacionales fue pronto denominador común en los diversos textos legislativos europeos en materia de protección de datos[34].

A los efectos de delimitar el concepto de "transferencia internacional de datos", debe señalarse que el mismo no viene definido como tal bajo la LOPD, que tan sólo se refiere a la misma en su artículo 3 c) como una de las operaciones de tratamiento de datos[35].

---

[30] El TJUE ha recordado su carácter de régimen especial, complementario, por lo tanto, del régimen general que establece el Capítulo II de la Directiva 95/46/CE relativo a la licitud de los tratamientos de datos. Sentencia del Tribunal de Justicia de la Unión Europea, de 6 de octubre de 2015, en el asunto C-362/14, fragmento número 46.

[31] Vid. DURÁN CARDO, Ana Belén, *La figura del responsable en el derecho a la protección de datos. Génesis y evolución normativa ante el cambio tecnológico y en perspectiva multinivel*, Universidad Autónoma de Barcelona, Barcelona, 2015, p. 312.

[32] Vid. GUASCH PORTAS, Vicente, ob. cit., p. 21 y 22.

[33] "A través de los derechos de acceso, rectificación, cancelación y oposición, también conocidos como "derechos ARCO", podemos saber qué información personal se está tratando por un responsable, de quién o de dónde se obtuvieron los datos y a quién se los ha cedido, modificar o rectificar errores, cancelar datos que no se deberían estar tratando u oponernos a tratamientos de datos personales realizados sin nuestro consentimiento". AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *El derecho fundamental a la protección de datos: guía para el ciudadano*, 2011, p. 22.

[34] Vid. REBOLLO DELGADO, Lucrecio, ob. cit., p. 72 y 73.

[35] La LOPD entiende por tratamiento de datos personales, al tenor de su artículo 3 c), aquéllas "*operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación (…), así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias".*

Así, será el artículo 5.1 letra s) del 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 adelante "Reglamento de la LOPD") el que se ocupe de tal cometido, entendiendo por "transferencia internacional de datos" todo "*tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo*[36]*, 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*" [37].

La mayoría de supuestos se caracterizan por la presencia de dos empresarios –de naturaleza pública o privada-, dentro de una misma estructura corporativa, produciéndose una centralización de datos del grupo de sociedades en la sede matriz, relativos a los empleados o a los clientes, o bien fuera de ella[38].

El régimen jurídico aplicable en España a toda transferencia internacional de datos se contiene en los artículos 33 y 34 de la LOPD, como instrumento de transposición en España de los artículos 25 y 26 de la Directiva 95/46/CE, y con los artículos 65 a 70 y 137 a 144 del Reglamento de la LOPD.

No toda transferencia internacional de datos es relevante para el ordenamiento jurídico español. La misma debe tener como objeto "datos personales"[39], entendidos como "*cualquier información concerniente a personas físicas identificadas o identificables*"[40], nacionales o extranjeras, registrados en "*soporte físico, que los haga susceptibles de tratamiento*"[41]. Como ha señalado el Tribunal Constitucional "el objeto de protección del derecho a la protección de datos no se reduce sólo a los datos íntimos

[36] Aunque la LOPD no se refiere en materia de transferencias internacionales de datos a los Estados miembros del EEE que no forman parte de la UE (en concreto, Islandia, Liechtenstein y Noruega), sino que se centra en los Estados miembros de la UE, si tenemos en cuenta lo indicado por la AEPD en sus resoluciones e Informes Jurídicos, ha de entenderse, por regla general, que las revelaciones de datos destinadas a las tres jurisdicciones del EEE anteriormente citadas, (…) no recaen bajo la definición de "transferencia internacional de datos" . Vid. CÁRDENAS ARTOLA, Ignacio; FERRERO RECASENS, Eduardo, entre otros, ob.cit., p. 12.

[37] Ello se pone en relación con el artículo 1.2 de la Directiva 95/46/CE, según el cual "Los Estados miembros no podrán restringir ni prohibir la libre circulación de datos personales entre los Estados miembros por motivos relacionados con la protección garantizada en virtud del apartado 1". Además, como apunta REBOLLO DELGADO, "en tanto que los datos constituyen bienes integrados en el sistema de libertad de la Unión, el concepto de transferencia internacional se refiere en exclusiva a los supuestos en los que el país de destino sea un tercer Estado no miembro de la Unión" Vid. REBOLLO DELGADO, Lucrecio, ob. cit., p. 73.

[38] Vid. SANCHO VILLA, Diana, *Transferencia internacional*, ob.cit., p. 40 y ss.

[39] Vid. Artículos 2 a) Directiva 95/46/CE, 3 a) de la LOPD y 5.1 f) del Reglamento de la LOPD.

[40] Vid. Artículo 3.1 a) de la LOPD.

[41] Vid. Artículo 2.1 de la LOPD.

de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por terceros pueda afectar a sus derechos, sean o no fundamentales, porque su objeto no es sólo la intimidad individual, que para ello está la protección que el artículo 18.1 CE otorga, sino los datos de carácter personal"[42].

Así, se encuentran en esta situación todos los datos contenidos en un "fichero", entendido como "*todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso"*[43], con independencia de que se encuentren en un soporte informático o no automático.

En lo que al ámbito de aplicación territorial de la LOPD se refiere, deseo subrayar que tan sólo resulta relevante aquélla transferencia efectuada en tres supuestos. En primer lugar, cuando la transferencia se efectúe en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento[44]. El requisito que la Ley exige es la tenencia de un establecimiento en España, que se traduce en "una vinculación económica efectiva y estable, y que puede concretarse jurídicamente mediante la tenencia en España de una sociedad (filial o no) o de una sucursal"[45].

> Resulta destacable la controversia generada a raíz de las múltiples reclamaciones que se han efectuado en relación con la responsabilidad de sucursales o filiales en España de entidades extranjeras que llevan a cabo tratamientos de datos personales no consentidos. Las filiales españolas de dichos buscadores entienden que no pueden responsabilizarse de los tratamientos de datos efectuados por sus matrices. Esta polémica ha dado lugar al planteamiento por parte de la AN de una cuestión prejudicial ante el TJUE, que deberá pronunciarse sobre la aplicabilidad de la normativa española de protección de datos a los tratamientos efectuados por una sociedad extranjera que simplemente tiene una oficina de representación comercial en nuestro país[46].

Del mismo modo, la Directiva 95/46/CE, señala que "*los Estados miembros aplicarán las disposiciones nacionales que haya aprobado para la aplicación de la presente Directiva a todo tratamiento de datos personales cuando (…) el tratamiento*

[42] Vid. Sentencia núm. 292/2000, de 30 de noviembre (Rec. 1463/2000), Fundamento Jurídico Sexto.
[43] Vid. Artículo 3.1 b) de la LOPD.
[44] "Hay que subrayar que esta regla despliega sus efectos respecto de los responsables del tratamiento y no respecto de los encargados. Puede suceder que el responsable establecido en el extranjero contrate los servicios de un agente establecido en España para que gestione sus datos o haga determinadas operaciones obre ellos (…). Las obligaciones del encargado se definen de acuerdo con la ley del responsable, sin perjuicio de las obligaciones que el Estado donde el encargado está establecido pueda imponerle de manera imperativa". SANCHO VILLA, Diana, "Protección de los datos personales y transferencia internacional: cuestiones de ley aplicable", *Revista Jurídica de Castilla y León*, nº 16, (2008), p. 411.
[45] Vid. SANCHO VILLA, Diana, ob. cit., p. 77.
[46] Vid. CÁRDENAS ARTOLA, Ignacio; FERRERO RECASENS, Eduardo, entre otros, ob.cit., p. 27.

sea efectuado en el marco de las actividades de un establecimiento del responsable del tratamiento en el territorio del Estado miembro"[47].

En consecuencia, señala SANCHO VILLA, "cuando el tratamiento se distribuye entre los distintos establecimientos de un responsable, localizados en Estados parte diferentes, en el marco de las actividades de cada uno de aquellos, será de aplicación la ley de cada uno de los Estados parte en cuestión"[48].

En segundo lugar, cuando al responsable del tratamiento y que, por lo tanto, efectúa la transferencia internacional de datos, sin hallarse en territorio español, le sea de aplicación la legislación española en aplicación de las normas de Derecho Internacional Público.

En tercer lugar y último lugar, se aplicará la LOPD cuando el responsable del tratamiento que efectúe la transferencia, sin estar establecido en territorio de la Unión Europea, utiliza en el tratamiento de datos medios situados en territorio español que presentan un carácter de permanencia, no utilizándose únicamente con *"fines de tránsito*"[49].

No obstante, no será de aplicación la LOPD en aquéllas transferencias internacionales de datos en relación con ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas –por ejemplo, un álbum de fotos familiar o una agenda de teléfonos-, a los ficheros sometidos a la normativa sobre protección de materias clasificadas[50] y a los ficheros establecidos para la investigación del terrorismo y de las formas graves de delincuencia organizada.

En otras palabras, apunta SANCHO VILLA, puede entenderse que integra una transferencia internacional de datos aquélla transmisión que suponga la salida "física" de los datos personales objeto de la LOPD del territorio español, al margen de que esa

[47] Vid. Artículo 4.1 a) de la Directiva 95/46/CE.
[48] Vid. SANCHO VILLA, Diana, ob. cit., p. 78.
[49] Con ello se evita que el responsable del tratamiento se sitúe con ánimo defraudatorio en un tercer Estado no miembro de la UE y que no reúna un nivel adecuado de protección, aprovechando su legislación más favorable, y recoja datos de personas físicas españolas mediante un servidor situado en España.
[50] Por materias clasificadas debemos entender a lo dispuesto en la Ley 9/1968, de 5 de abril, sobre secretos oficiales, que indica que podrán ser declaradas materias clasificadas los asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas pueda dañar o poner en riesgo la seguridad y defensa del Estado (artículo 2). La calificación de una materia como clasificada corresponde exclusivamente al Consejo de Ministros y a la Junta de Jefes de Estado Mayor (artículo 4).

transmisión suponga también la salida "jurídica" en el sentido de pérdida de competencia de la ley española. De este modo, hay que tener en cuenta que no se produce esta salida jurídica –aunque sí física- cuando el receptor de los datos establecido en el extranjero es un mero encargado de tratamiento"[51].

El Tribunal de Justicia de la Unión Europea ha venido reformulando el concepto que venimos analizando. De especial interés resulta la Sentencia "Lindqvist", de 6 de noviembre de 2003 (Asunto C-101/01-Bodil Lindqvist)[52], referente a la publicación de datos personales en Internet. El TJUE debía determinar si la difusión de datos personales en una web, de manera que resultan accesibles a personas que se encuentran en un país tercero, constituye una "transferencia internacional de datos" del artículo 25 de la Directiva 95/46/CE. Finalmente, el Tribunal respondió de forma negativa a esta cuestión, pues para que exista "transferencia" es esencial que "exista cierto movimiento de datos de carácter personal"[53].

II. REQUISITO ESENCIAL DE VALIDEZ DE LA TRANSFERENCIA INTERNACIONAL DE DATOS: CUMPLIMIENTO DE LA LOPD Y DEL REGLAMENTO DE LA LOPD

Toda transferencia internacional de datos por parte de un responsable establecido en España[54] debe cumplir con las exigencias de la normativa de protección de datos, del mismo modo que si la transmisión se efectuase en el marco del territorio español o con destino a un Estado que garantice un nivel de protección adecuado. Ya el artículo 25.1 de la Directiva 95/46/CE dispone que las mismas tan sólo puedan efectuarse cuando "*sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas*

[51] Vid. SANCHO VILLA, Diana, ob. cit., p. 26.

[52] Vid. ORTEGA GIMÉNEZ, Alfonso, *Internet, publicación de datos personales y transferencias internacionales de datos: la sentencia del TJCE "Lindqvist", de 6 de noviembre de 2003*, Aranzadi Bibliotecas, 2009 y también DE MIGUEL ASENSIO, Pedro Alberto, Protección de datos personales, Ed Aranzadi, Madrid, p. 34 y ss.

[53] Como dice ORTEGA GIMÉNEZ, "parece evidente que el TJUE optó por la "solución más fácil", (…) pues teniendo en cuenta el estado de desarrollo de Internet en el momento de elaboración de la Directiva, (…) el legislador comunitario no tenía la intención de incluir en el concepto (…) la difusión de datos en una página web, ni siquiera cuando estos últimos resulten accesibles a personas de países terceros". ORTEGA GIMÉNEZ, Alfonso, *La (des)protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita*, Agencia Española de Protección de datos, Madrid, 2014, p. 25.

[54] Pues la ley española es competente para regir el acto de transmisión al extranjero de los datos protegidos por la LOPD en las transferencias internacionales promovidas desde España.

con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado". En la misma línea, en artículo 33.1 de la LOPD permite la realización de transferencias internacionales de datos cuando, "*además de haberse observado lo dispuesto en (la LOPD), se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas*".

1. Creación de un fichero de titularidad privada.

En efecto, el empresario creará con toda probabilidad un fichero de titularidad privada que deberá ser notificado a la Agencia de Protección de Datos, con carácter previo a la creación del mismo[55]. En la notificación deberán precisarse los elementos del artículo 26.2 de la LOPD y del artículo 55.2 del Reglamento de la LOPD. En concreto, la LOPD señala que debe informarse a la AEPD de "*las transferencias de datos que se prevean a países terceros*", y el Reglamento de la LOPD añade la exigencia de notificar "*los destinatarios de cesiones y transferencias internacionales de datos*"[56]. Si la notificación se ajusta a los requisitos legales y reglamentarios, el Registro General de Protección de Datos inscribirá el fichero[57].

No obstante, el responsable del tratamiento no tiene la obligación de conocer, en el momento de la notificación a la AEPD su propósito de crear un fichero, el número de transferencias internacionales de datos que pretende realizar y los destinatarios de las mismas. Por ello, si la decisión de transmitir los datos a otro país es posterior a la inscripción del fichero en el Registro, el responsable del tratamiento deberá notificarlo a la AEPD, en aplicación del artículo 26.3 de la LOPD.

---

[55] Vid. Artículo 26.1 de la LOPD.

[56] El conocimiento del país destinatario de las transferencias internacionales de datos por parte de la AEPD no supone la introducción de ningún control previo y alternativo a la necesidad de autorización que contempla el art. 33.1 LOPD.

[57] Para realizar la inscripción inicial del fichero y, en su caso, la posterior modificación o supresión de la inscripción, se encuentra disponible en la Sede Electrónica de la Agencia Española de Protección de Datos el Servicio Electrónico NOTA a través del que deberán efectuarse las solicitudes de inscripción de ficheros en el Registro General de Protección de Datos (aprobado mediante Resolución de la AEPD de 12 de julio de 2006- B.O.E. 181 de 31 de julio). AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Inscripción de ficheros, en línea: https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/index-ides-idphp.php [consultado el 29.02.2016].

2. El régimen de la cesión o comunicación de datos.

Una transmisión de datos personales interna, cuyo destino se circunscribe al territorio español, se somete al régimen de la "cesión o comunicación de datos", definida 3.1 i) de la LOPD como "*toda revelación de datos realizada a una persona distinta del interesado*" y regulada en el artículo 11 de la misma Ley. Así, cabe destacar que los interesados deben ser informados de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información; de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, entre otros elementos[58]. Cuando la transferencia de datos se efectúe a terceros países, además de cumplirse con estas exigencias, deberán reforzarse[59].

La LOPD impone el deber de informar a los afectados por la transmisión de los datos tanto al empresario cedente como al cesionario de los datos. No obstante, la obligación del cedente presenta un carácter más rígido, pues el mismo debe informar a los afectados con carácter previo a la realización de la primera transmisión de datos de carácter personal. Al tenor del artículo 27 de la LOPD, el responsable del fichero que actúe como cedente "*deberá informar de ello a los afectados, indicando, asimismo, la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario*".

Por el contrario, el cesionario, al haber obtenido datos de carácter personal que no han sido recabados del interesado –cumpliéndose por lo tanto el presupuesto del artículo 5.4 de la LOPD- tiene el deber de informar de forma "*expresa, precisa e inequívoca*" al titular de los datos en el plazo máximo de 3 meses, a contar desde el momento del registro de los datos salvo que, como apunta el artículo 5.4 de la LOPD, el mismo "*ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1*" del artículo en cuestión.

[58] Vid. Artículo 5.1 de la LOPD.

[59] "El empresario responsable del tratamiento debe cumplir con el deber de información al interesado en el marco de las cesiones internas de datos del art. 11 LOPD, la transferencia de datos al extranjero necesitará que se refuerce el cumplimiento de esas obligaciones". SANCHO VILLA, Diana, *Transferencia internacional*, ob.cit., p. 88.

Y es que no debe olvidarse la estrecha conexión que existe entre el derecho a la información del que goza el interesado y el efectivo ejercicio de su derecho a consentir. Ello ya lo afirmó el Tribunal Constitucional en la famosa Sentencia núm. 292/2000, de 30 de noviembre[60], señalando que "*es evidente que el interesado debe ser informado tanto de la posibilidad de cesión de sus datos personales y sus circunstancias como del destino de éstos, pues sólo así será eficaz su derecho a consentir, en cuanto facultad esencial de su derecho a controlar y disponer de sus datos personales*"[61].

Si atendemos al régimen de las comunicaciones o cesiones de datos personales del artículo 11.1 de la LOPD, toda comunicación de datos deberá llevarse a cabo para el "*cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado*"[62]. A lo que se añade la exigencia del artículo 6.1 de la LOPD, según la cual "*el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado*[63]*, salvo que la ley disponga otra cosa*".

Teniendo presente que las transferencias internacionales de datos son cesiones de datos que, en sí, suponen un "tratamiento de los datos de carácter personal", al igual que la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación

---

[60] Vid. Sentencia del Tribunal Constitucional (Pleno) núm. 292/2000, de 30 de noviembre (RTC\2000\292), Fundamento Jurídico 13º.

[61] "Para lo que no basta que conozca que tal cesión es posible según la disposición que ha creado o modificado el fichero, sino también las circunstancias de cada cesión concreta. Pues en otro caso –prosigue el TC- sería fácil al responsable del fichero soslayar el consentimiento del interesado mediante la genérica información de que sus datos pueden ser cedidos. De suerte que, sin la garantía que supone el derecho a una información apropiada mediante el cumplimiento de determinados requisitos legales (art. 5 LOPD) quedaría sin duda frustrado el derecho del interesado a controlar y disponer de sus datos personales, pues es claro que le impedirían ejercer otras facultades que se integran en el contenido del derecho fundamental al que estamos haciendo referencia". Vid. Sentencia del Tribunal Constitucional (Pleno) núm. 292/2000, de 30 de noviembre (RTC\2000\292), Fundamento Jurídico 13º.

[62] Ello también lo remarca el artículo 10.1 del Reglamento de la LOPD.

[63] "Al analizar las conductas relativas al consentimiento es preciso mencionar también una cuestión (…). Se trata de la dificultad con la que se encuentran los responsables de los sitios de Internet a la hora de verificar de forma fehaciente la identidad de un usuario (…). También sería necesario reflexionar sobre el valor de un consentimiento otorgado por una persona cuya identidad, al fin y a al cabo, no conocemos con un razonable margen de seguridad (…). El problema se pone claramente de manifiesto en el caso de los menores, ya que se dan de alta en sus servicios (de los prestadores de servicios de la sociedad de la información), lo que deja sin efecto muchas de las previsiones de la normativa de protección de datos y, en particular, las relativas a la capacidad para prestar el consentimiento (…). Desde el punto de vista democrático, una regulación excesivamente proteccionista, dirigida a ciudadanos que sitúan su privacidad por debajo no ya de otros valores, sino de simples ventajas en comodidad o económicas, podría verse como la defensa a ultranza de derechos que no han sido reinterpretados en el nuevo contexto tecnológico y que han dejado –o están dejando- de contar con un apoyo social que justifique su existencia". BALERO TORRIJOS, Julián, *La Protección de los Datos Personales en Internet ante la Innovación Tecnológica*, Ed. Thomson Reuters Aranzadi, Navarra, 2013, p. 181 y ss.

de los datos, cuando el responsable del tratamiento efectúe la recogida de datos –que ya supone tratamiento de los mismos-, se exigirá un primer consentimiento del interesado.

Si en la finalidad de dicho tratamiento ya se incorpora la transmisión internacional de los datos recogidos[64], se requerirá la concurrencia de dos consentimientos, por más que se superpongan. Es más, como se explicará más adelante, incluso puede que se requiera un tercer consentimiento, si la transferencia internacional se dirige a un país que no ofrece un nivel de protección equiparable a la LOPD, como excepción prevista en el artículo 34 d) de la LOPD según la cual el consentimiento inequívoco a la transferencia del afectado exonera al responsable del tratamiento de la obtención de la autorización previa del Director o Directora de la AEPD.

Si bien el consentimiento del interesado opera con carácter general en las cesiones de datos, la LOPD y su Reglamento establecen un conjunto de excepciones a la misma[65]. Resulta de interés la excepción por la cual no resulta necesario recabar el consentimiento del interesado cuando se trate de datos recogidos de fuentes accesibles al público. Dado que en la actualidad, por "fuentes accesibles al público", cabe entender una gran variedad de supuestos –piénsese en la cantidad de información que se publica en las redes sociales-, el artículo 3 j) de la LOPD, después de definir el término[66], enuncia con carácter de *numerus clausus* las cuatro fuentes de acceso público que se regirán por el estatus jurídico del artículo 11.2 de la LOPD: en primer lugar, "*el censo promocional*"; en segundo lugar, "*los repertorios telefónicos en los términos previstos por su normativa específica*"; en tercer lugar, "*las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo*" y, por último, "*los diarios y boletines oficiales y los medios de comunicación*". Por lo tanto, no cabe entender por "fuente accesible al público" la información que se publique en redes sociales como Facebook.

[64] El interesado debe conocer la finalidad para que se recogen los datos, y si en la misma se incluye la transferencia internacional de datos, éste debe saber finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar. De lo contrario, el artículo 11.3 de la LOPD declara la nulidad del cuando la información que se facilite al interesado no le permita conocer dicha finalidad.

[65] Vid. Artículo 11.2 de la LOPD y artículo 10 del Reglamento de la LOPD.

[66] Por fuentes accesibles al público se entiende "aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación"

III. ÁMBITO SUBJETIVO DE LA TRANSFERENCIA INTERNACIONAL DE DATOS.

Desde una perspectiva subjetiva, resulta esencial determinar qué partes pueden intervenir o se pueden hallar afectadas en el marco de una transferencia internacional de datos.

En toda transferencia internacional de datos intervienen dos personas: por una parte, el "exportador de datos personales", que es "*la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realice, conforme a lo dispuesto en el presente Reglamento, una transferencia de datos de carácter personal a un país tercero*"[67] y, por otra parte, el "importador de datos personales", como "*la persona física o jurídica, pública o privada, u órgano administrativo receptor de los datos en caso de transferencia internacional de los mismos a un tercer país, ya sea responsable del tratamiento, encargada del tratamiento o tercero*"[68]. Y, tendiendo presente que la transferencia siempre se va a referir a datos personales concernientes a una persona física identificada o identificable –que el artículo 3 e) de la LOPD denomina "afectado o interesado"-, ésta siempre gozará de ciertos derechos en el marco de esta transferencia.

A su vez, la LOPD distingue entre el "responsable del fichero o del tratamiento" y el "encargado del tratamiento". Cuando la persona física o jurídica decide sobre la finalidad, contenido y uso del tratamiento de los datos de carácter personal, se le denomina "responsable del fichero o del tratamiento"[69]. Si por el contrario, dicha persona no asume tal control sobre los datos, sino que los trata por cuenta del responsable del tratamiento, al mantener una relación jurídica para con el mismo que delimita su ámbito de actuación para la prestación de un servicio, se le denomina "encargado del tratamiento"[70].

Además, el Reglamento de la LOPD añade otra tipología de sujeto que se puede hallar en el marco de una transferencia internacional de datos personales, que es el "tercero"[71], cuyo concepto se define de forma negativa, como toda persona física o

[67] Vid. Artículo 5.1 j) del Reglamento de la LOPD.
[68] Vid. Artículo 5 ñ) del Reglamento de la LOPD.
[69] Vid. Artículo 3 d) de la LOPD y artículo 5.1 q) del Reglamento de la LOPD.
[70] Vid. Artículo 3 g) de la LOPD y artículo 5.1 i) del Reglamento de la LOPD.
[71] Vid. Artículo 5.1 r) del Reglamento de la LOPD.

jurídica "*distinta del afectado o interesado, del responsable del tratamiento, del responsable del fichero, del encargado del tratamiento y de las personas autorizadas para tratar los datos bajo la autoridad directa del responsable del tratamiento o del encargado del tratamiento*"[72].

Las transferencias internacionales de datos pueden ser entre responsables del tratamiento, entre un responsable del tratamiento y un encargado del tratamiento, y también de un encargado a un subencargado del tratamiento.

En el primer caso se produce una pérdida de la competencia de la ley española, pues se está ante una situación que no encaja en ningún presupuesto de los establecidos en el artículo 2.1 de la LOPD, a no ser que el responsable del tratamiento que actúe como importador de los datos le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público o utilice en el tratamiento de datos medios situados en territorio español[73], salvo que tales medios se utilicen únicamente con fines de tránsito.

En el segundo caso, cuando la transferencia se efectúa a un encargado del tratamiento que se encuentra en un tercer Estado no miembro de la UE, realmente no se produce esta pérdida de competencia de la ley española, y ello porque el responsable del tratamiento que actúa como exportador de los datos en un establecimiento situado en el territorio español es quien realmente posee el control y dominio sobre los datos, decidiendo sobre su finalidad, contenido y uso. Así, el encargado del tratamiento que actúa como importador de los datos y que se encuentra en un Estado no miembro de la UE, permanece sometido a la ley española. Como apunta SANCHO VILLA, "aunque el

[72] "El concepto de tercero se incluyó en la Propuesta de Directiva de 1992 a raíz de la enmienda 134ª propuesta por el Parlamento Europeo que se inspiró en la Ley federal alemana de 1990. La Comisión entendió que debía utilizarse para delimitar la figura del cesionario o quien recibe la comunicación de datos (…). Se confirmó (…) que la utilidad del concepto era incorporar a aquellos sujetos que estuvieran fuera del círculo de influencia del responsable (…) asimilándose al concepto de tercero del derecho civil, como sujeto que no es parte de una relación jurídica determinada, normalmente la que existirá entre el responsable del tratamiento y el interesado. DURÁN CARDO, Ana Belén, La figura del responsable en el derecho a la protección de datos. Génesis y evolución normativa ante el cambio tecnológico y en perspectiva multinivel, Universidad Autónoma de Barcelona, Barcelona, 2015, p. 301 y ss.

[73] Por ejemplo, ello sucedería cuando un empresario establecido en un Estado no perteneciente a la UE realizase actuaciones que supongan la colocación de cookies en el ordenador del usuario que se conecta a la página web de aquel, o la descarga de *javascript* por parte de este usuario para acceder a los contenidos de la página, mediante los cuales el empresario recabe datos personales para tratamiento. El responsable del tratamiento debería designar representante en España (art. 5.1 LOPD) y definir claramente la finalidad de la recogida de los datos (en el caso de una cookie, el interesado debería poder aceptar su colocación o no), asegurar que los datos recabados son adecuados y no excesivos con relación a esa finalidad y que se han adoptado medidas de seguridad suficientes. SANCHO VILLA, Diana, *Transferencia internacional*, ob.cit., p. 98.

tratamiento no se realice en España, sí se entiende que pertenece a la esfera de las actividades del establecimiento del responsable –considerando 18 *in fine* Directiva-. Aunque el tratamiento no se realice físicamente en España, sí se entiende que el mismo se desarrolla dentro del marco de actividades del establecimiento en España del responsable del tratamiento, no provocando pérdida de la competencia de la ley española"[74].

Ejemplo de esta segunda tipología de transferencias son los "contratos de administración y gestión de ficheros y datos ajenos"[75] y los "contratos de explotación económica de datos personales con finalidades de prospección comercial"[76].

Por último, cabe que una transferencia internacional de datos se realice entre un encargado del tratamiento que actúa como exportador de los datos, establecido en España, y un subencargado del tratamiento que actúa como importador de los datos, y que se halla ubicado en un país tercero que no garantiza un nivel adecuado de protección. Dado que el encargado exportador no puede decidir de forma autónoma sobre la finalidad de los datos, se requiere la existencia de un contrato marco entre éste y el responsable del tratamiento en el que éste autorice la subcontratación y la transferencia internacional de datos[77].

---

[74] Vid. SANCHO VILLA, Diana, *Transferencia internacional,* ob.cit., p. 97.

[75] El tratamiento de datos derivado de este negocio es el supuesto más usual de contrato de *outsourcing*, mediante el cual el proveedor o encargado (*outsourcer*) va a arrendar la prestación de un determinado servicio de administración, gestión o conservación de los ficheros y datos, a cambio del precio que satisfaga el responsable del tratamiento o arrendatario. SANCHO VILLA, Diana, *Transferencia internacional de datos personales*, Agencia de Protección de Datos, Madrid, 2003, p. 51 y 52.

[76] Es frecuente el contrato de arrendamiento de datos, mediante el cual la empresa responsable del tratamiento dedicada a recabar datos personales con fines de prospección comercial (por ejemplo de fuentes públicas), consiente a cambio de precio, el uso de los datos personales que obran en su poder de acuerdo con unos determinados perfiles solicitados por la empresa arrendataria (que actúa como encargada), comprometiéndose a la entrega de los listados resultantes para una concreta finalidad que normalmente se circunscribirá a una determinada campaña de publicidad. SANCHO VILLA, Diana, *Transferencia internacional de datos personales,* Agencia de Protección de Datos, Madrid, 2003, p. 51 y 52.

[77] Vid. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Transferencias internacionales de datos*, Autorización de la Directora de la Agencia Española de Protección de Datos, en línea: https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides-idphp.php [consultado el 1.03.2016].

IV. ÁMBITO OBJETIVO DE LA TRANSFERENCIA INTERNACIONAL DE DATOS.

1. Las transferencias a terceros Estados que garantizan un "nivel de protección adecuado": la norma general.

En primer término, debe señalarse que, mientras que no existe restricción alguna en relación con las transferencias de datos personales efectuadas entre países miembros del Área Económica Europea, en lo que a las transferencias internacionales de datos se refiere existe una regla general, contenida en el artículo 33.1 de la LOPD: "*No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley".* Asimismo, dicho precepto transpone lo dispuesto en el artículo 25.1 de la Directiva 95/46/CE, según el cual únicamente pueden efectuarse trasferencias internacionales de datos 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*"[78].

El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará, al tenor del artículo 25.2 de la Directiva 95/46/CE y del artículo 33.2 de la LOPD atendiendo a "*todas las circunstancias que concurran en una transferencia o categoría de transferencias de datos*". A título ilustrativo, dichos preceptos enumeran los criterios[79] a los que deberá atenderse para determinar el nivel de protección del país tercero: "*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*

[78] Como se expone en la web de la AEPD, debe recordarse que en el caso de que la transferencia internacional de datos con destino a uno de estos países sea consecuencia de una prestación de servicios, esta circunstancia no exime de la obligación de tener que suscribir un contrato conforme a lo dispuesto en el artículo 12 de la LOPD. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *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 18.03.2016].

[79] "Como indica Jessica MATUS ARENAS, los perjuicios económicos que pueden derivarse de la limitación que establece el artículo 25 de la Directiva (…) obliga a fijar o determinar con precisión qué es lo que exigir la Directiva con el requisito de "protección adecuada". En este punto es imprescindible efectuar el análisis del Documento de Trabajo WP12 del Grupo de Trabajo creado al amparo del artículo 29 de la Directiva. GUASCH PORTAS, Vicente, "La transferencia internacional de datos de carácter personal", *Revista de Derecho UNED*, núm. 11, (2012), p. 423.

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" –añadiéndose en la LOPD "*el contenido de los informes de la Comisión de la Unión Europea*".

Los instrumentos por los que se puede materializar la declaración del nivel de protección adecuado son variados y presentan distinta naturaleza[80]. En primer lugar, hallamos los actos de carácter público, ya sean internacionales –por ejemplo, las Directrices de la OCDE, de la ONU o del Convenio 108/81/CE-, comunitarios y/o estatales. En segundo lugar hallamos los actos de carácter privado, mediante los denominados "contratos-tipo" o las "normas corporativas vinculantes".

La Comisión Europea y, en España, la Agencia de Protección de Datos, asumen un papel central en este procedimiento. Por una parte, la Directiva 95/46/CE faculta a la Comisión Europea para hacer constar que un país tercero garantiza un nivel de protección adecuado, "*a la vista de su legislación interna o de sus compromisos internacionales*". Además, los Estados miembros y la Comisión deben informarse recíprocamente cuando estimen que un tercer país no garantiza un nivel adecuado de protección y, para el caso que la Comisión compruebe que un tercer país no lo garantiza, serán los Estados miembros quiénes deberán adoptar las medidas necesarias para impedir cualquier transferencia de datos personales al tercer país de que se trate, pudiendo la Comisión iniciar negociaciones destinadas a remediar dicha situación.

Por otra parte, el artículo 33.2 de la LOPD faculta a la Agencia Española de Protección de Datos (en adelante, "AEPD") para evaluar el nivel de protección que ofrece el país de destino de la transferencia internacional de datos, atendiendo a los criterios antes expuestos. Además, en virtud del artículo 37.1 l) de la LOPD la AEPD ejerce "*el control y adopta las autorizaciones que procedan en relación con los movimientos internacionales de datos*". Ello cabe ponerlo en relación con el artículo 18 y ss. Directiva 95/46/CE, que establece la obligación de notificación a la autoridad de

[80] Vid. ORTEGA GIMÉNEZ, Alfonso, *La (des)protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita*, Agencia Española de Protección de datos, Madrid, 2014, p. 31.

control con anterioridad a la realización de un tratamiento o un conjunto de tratamientos destinados a la consecución de un fin o de varios fines conexos[81].

Asimismo, el artículo 21 de la Directiva 95/46/CE configura el deber de Estados miembros de establecer que la autoridad de control lleve un registro de los tratamientos notificados. Por ello, el artículo 39 de la LOPD crea el Registro General de Protección de Datos, como órgano integrado en la Agencia de Protección de Datos, estableciendo que serán objeto de inscripción, "*las autorizaciones a que se refiere la presente Ley*" y "*los códigos tipo a que se refiere el artículo 32 de la presente Ley*", entre otros elementos.

Si únicamente existiese la regulación prevista en el artículo 25.1 de la Directiva 95/46/CE o en el artículo 33.1 de la LOPD, el movimiento de datos hacia el exterior de la Unión sería extremadamente limitado[82], lo cual resulta inviable para cualquier economía moderna[83]. Así, tan sólo podrían realizarse transferencias internacionales de datos desde el AEE con destino a los países que, en virtud de las decisiones de la Comisión Europea o de la AEPD, garantizasen un nivel adecuado de protección[84].

---

[81] Deberá figurar en la notificación: el nombre y la dirección del responsable del tratamiento y, en su caso, de su representante; el o los objetivos del tratamiento; una descripción de la categoría o categorías de interesados y de los datos o categorías de datos a los que se refiere el tratamiento; los destinatarios a los que se pueden comunicar los datos; las transferencias de datos previstas a países terceros y una descripción general que permita evaluar si las medidas adoptadas resultan adecuadas para garantizar la seguridad del tratamiento. Artículo 19.1 de la Directiva 95/46/CE.

[82] Vid. GUASCH PORTAS, Vicente, ob. cit., p. 22.

[83] En relación con el concepto de "economía moderna", señalar que "la mundialización actúa como catalizador de un conjunto de cambios productivos. La liberalización del comercio internacional y del movimiento de capitales, la disminución de los costes del transporte y de las comunicaciones están acelerando la tendencia histórica hacia el aumento de la división del trabajo. Y las empresas se están adaptando al nuevo contexto, reestructurando sus actividades productivas a nivel mundial.
Los cambios en la división internacional del trabajo responden a la incorporación a la economía global de países en vías de desarrollo y, por otro lado, a cambios en la tecnología, el transporte y el comercio que permiten a muchas empresas colocar su producción en diversos lugares del mundo, como consecuencia de lo que se ha denominado "fragmentación de la cadena del valor" y, también, "desintegración de la producción".
Ahora es más fácil que nunca, como consecuencia de la desregulación y de la oportunidad de menores costes, situar cada fase de la "cadena del valor" de la producción en el lugar que ofrezca mejores ventajas en términos de costes laborales, fiscales o medio-ambientales. El caso de la elaboración de la muñeca *Barbie* es un ejemplo de tal fragmentación productiva: el diseño y la pintura son norteamericanos, los cabellos y el plástico se hacen en Japón y Taiwán, la ropa es china y el montaje se lleva a cabo en Indonesia y Malasia. Vid. ZUFIAUR NARVAIZA, José María, "Globalización económica y deslocalizaciones productivas", *Relaciones laborales: Revista crítica de teoría y práctica*, nº 1, (2005), p. 1161.

[84] Hasta la fecha han sido declarados como países con nivel adecuado de protección los siguientes: 1) Suiza (Decisión 2000/518/CE de la Comisión, de 26 de julio de 2000); 2) 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); Argentina (Decisión 2003/490/CE de la Comisión, de 30 de junio de 2003); Guernsey (Decisión 2003/821/CE de la Comisión, de 21 de noviembre de 2003); Isla de

Es por ello que tanto el artículo 26 de la Directiva 95/46/CE como el artículo 34 de la LOPD establecen un conjunto de excepciones a la regla general.

2. Transferencias a terceros Estados que no garantizan un "nivel de protección adecuado"

En efecto, pueden llevarse a cabo transferencias internacionales de datos a terceros Estados que no garantizan un "nivel de protección adecuado", pero que se hallen amparadas por alguna de las excepciones legalmente previstas, o bien cuando medie autorización del Director o Directora de la AEPD, siempre que previamente se haya cumplido lo dispuesto en la LOPD, y medien garantías adecuadas[85].

2.1 . Excepciones a la regla general previstas por la Directiva 95/46/CE y la LOPD.

Cabe señalar que, respecto las excepciones previstas en el artículo 26 de la Directiva 95/46/CE, cabe que los Estados miembros establezcan disposiciones de Derecho nacional contrarias a las mismas, para casos particulares.

Para la mejor comprensión del conjunto de excepciones y a los efectos de tratar la regulación de modo unitario, se señalará, en primer lugar, el conjunto de excepciones que son comunes tanto en la Directiva 95/46/CE como en la LOPD, para proseguir con la concreción de las especificidades previstas en ambos instrumentos.

La exigencia de que el país tercero proporcione un nivel de protección adecuado no será de aplicación, de acuerdo con la Directiva 95/46/CE y la LOPD:

- Cuando el afectado (o interesado de acuerdo con Directiva 95/46/CE) haya dado su consentimiento inequívoco a la transferencia prevista[86].

Man (Decisión 2004/411/CE de la Comisión, de 28 de abril de 2004); Jersey (Decisión 2008/393/CE de la Comisión, de 8 de mayo 2008); Islas Feroe (Decisión 2010/146/UE de la Comisión, de 5 de marzo de 2010); Andorra (Decisión 2010/625/UE de la Comisión, de 19 de octubre de 2010); Israel (Decisión 2011/61/UE de la Comisión, de 31 de enero de 2011); Uruguay (Decisión 2012/484/UE de la Comisión, de 21 de agosto de 2012); Nueva Zelanda (Decisión 2013/65/UE de la Comisión, de 19 de diciembre de 2012). AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *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 18.03.2016].

[85] Vid. ORTEGA GIMÉNEZ, Alfonso, *La (des)protección del titular,* ob.cit., p. 31.

[86] "Lo más destacable a nuestro juicio es la falta de unanimidad que se observa en la ciudadanía sobre la importancia de la privacidad. Esta es al menos la conclusión de los estudios realizados en el Observatorio Aragonés de la Sociedad de la Información (OASI) (…). El hecho de que haya muchos ciudadanos para

- ❖ Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado.
- ❖ Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero.
- ❖ Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público (en la Directiva 95/46/CE se añade el calificativo "importante", y no en la LOPD).
- ❖ Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- ❖ Cuando la transferencia se efectúe, a petición de la persona con interés legítimo, desde un Registro público y aquélla sea acorde con la finalidad del mismo.

Así, mientras que la Directiva 95/46/CE establece como excepción el que la "*transferencia sea necesaria para la salvaguardia del interés vital del interesado*", la LOPD establece como excepción el que "*la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios*"[87], sin determinar el sujeto beneficiario de dicha transferencia.

---

los que el bien jurídico directamente protegido tiene escaso valor (la protección de los datos), sobre todo cuando se confronta con otros posibles beneficios, propicia que las iniciativas empresariales más agresivas en materia de protección de datos encuentren siempre un amplio nicho entre la población que las acepta de forma acrítica, permitiendo de esta forma que se consoliden (…). Este carácter lábil de las actitudes de los ciudadanos se debe a la inexistencia, al menos en amplios sectores de población, de unas convicciones arraigadas y mayoritarias que den lugar a que los individuos realicen un esfuerzo de análisis previo a la prestación del consentimiento. Sin embargo, esta reflexión resulta especialmente importante, ya que el consentimiento que se presta en materia de protección de datos tiene un marcado componente ideológico, es decir, está relacionado con las opiniones y las actitudes. Es así porque, a diferencia de lo que ocurre con los consentimientos vinculados a otros derechos –como sería, por ejemplo, el caso de la propiedad-, las consecuencias prácticas y, en particular las económicas, asociadas a una u otra opción, aparecen lejanas o muy difuminadas, o simplemente no son percibidas por los ciudadanos. Característica esta que se acentúa todavía más si damos por cierto el hecho que, (…), los ciudadanos no son aún conscientes (…) del valor económico de su información personal". BALERO TORRIJOS, Julián, ob.cit., p. 170 y ss.

[87] Las transferencias que se vayan a legitimar en base a esta excepción, deben referirse al interés personal del interesado y, por ejemplo, no podrían encuadrarse bajo la misma las transferencias cuya finalidad fuese la investigación médica general. Sí se encuadraría, a título ilustrativo, una "transferencia de datos por parte de un médico establecido en España con vistas a la prestación de asistencia médica urgente cuando el sujeto se encuentre de viaje en un país que no proporciona un nivel de protección de datos adecuado". CÁRDENAS ARTOLA, Ignacio; FERRERO RECASENS, Eduardo, entre otros, *Memento experto. Protección de datos*, Ed. Francis Lefebvre, Madrid, 2012, p. 130.

En cuanto a las excepciones previstas por la LOPD, y no por la Directiva 95/46/CE, señalar que la regla general no será de aplicación, en primer lugar, "*cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España*"[88]; en segundo lugar, "*cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional*"; y, en tercer lugar, "*cuando se refiera a transferencias dinerarias conforme a su legislación específicas*".

Erróneamente, la LOPD establece, en su última excepción a la regla general, el supuesto en que precisamente se cumple la regla general. En efecto, establece como excepción el que la "*transferencia tenga como destino un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado*". Además, también resulta erróneo el establecer como excepción el que la "*transferencia tenga como destino un Estado miembro de la Unión Europea*", pues en este caso no nos hallaríamos ante una transferencia internacional de datos.

Como se expone en la página web de la AEPD, si la transferencia internacional de datos se ampara en alguno de los supuestos de excepción previstos en los apartados a) a j) del artículo 34 de la LOPD –los detallados con anterioridad-, o cuando el Estado en el que se encuentre el importador ofrezca un nivel adecuado de protección, igualmente el responsable del tratamiento deberá notificar dicha transferencia al Registro General de Protección de Datos para su inscripción a través de sistema NOTA de notificación de ficheros[89].

2.2.La presentación de "garantías suficientes" por el responsable del tratamiento de datos de carácter personal: autorregulación

Resulta especialmente relevante la excepción del artículo 33.1 de la LOPD, según la cual no podrán realizarse transferencias internacionales de datos personales con destino a países que no proporcionen un nivel de protección equiparable a la LOPD, "*salvo que,*

[88] Por ejemplo, España es parte del Convenio 108 del Consejo de Europa, relativo a protección de datos personales. Así, las transferencias internacionales a países terceros que no ofrezcan un nivel adecuado de protección que han ratificado el Convenio en cuestión se hallarán exentas de la autorización del Director/a de la AEPD.

[89] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Elaboración de Códigos Tipo. Objeto y naturaleza, en línea: https://www.agpd.es/portalwebAGPD/canalresponsable/elaboracion_codigos_tipo/index-ides-idphp.php [consultado el 16.03.2016].

además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas"[90].

Se considera que se aportan "garantías adecuadas" en dos supuestos: por una parte, cuando se celebra un contrato escrito entre el exportador y el importador de los datos en el que consten las necesarias garantías de respeto de los derechos y libertades de los sujetos afectados por las transferencias[91]; por otra parte, cuando en el seno de grupos multinacionales de empresas se emplean normas corporativas vinculantes, conocidas como "*Binding Corporate Rules"*, en que constan las mencionadas garantías de respeto del derecho fundamental a la protección de los datos personales de los sujetos afectados[92].

2.2.1. Cláusulas contractuales tipo

El responsable del tratamiento puede suministrar las "garantías adecuadas" que se exigen en el art. 33.1 de la LOPD a partir de instrumentos clásicos como es el Derecho contractual. Cuando el destinatario de los datos está establecido en un tercer Estado que carece de una normativa de protección equivalente a la del Estado de origen, la integración de ese vacío mediante cláusulas contractuales aparece como un instrumento particularmente idóneo para posibilitar una transferencia que de otro modo no estaría permitida[93].

Al tenor del artículo 70.2 del Reglamento de la LOPD, se entiende que el responsable del fichero o tratamiento otorga garantías adecuadas si aporta un contrato escrito perfeccionado entre el exportador y el importador en el que consten "*las necesarias garantías de respeto a la protección de la vida privada de los afectados y a sus derechos y libertades fundamentales y se garantice el ejercicio de sus respectivos derechos*".

---

[90] "Buena parte de las políticas públicas de protección de la vida privada vigentes en la generalidad de los Estados desarrollados optan por fórmulas de protección deducidas de os propios particulares, por entender que este tipo de modelo de reglamentación privada resulta más atractivo para los operadores, al ajustarse a las necesidades técnicas de un concreto sector de una manera más precisa y efectiva". SANCHO VILLA, Diana, *Transferencia internacional*, ob.cit., p. 64.

[91] Vid. Artículo 70.2 del Reglamento de la LOPD.

[92] Vid. Artículo 70.4 del Reglamento de la LOPD.

[93] SANCHO VILLA, Diana, *Transferencia internacional de datos personales,* Agencia de Protección de Datos, Madrid, 2003, p.70.

A tal efecto, tanto la Comisión Europea como la AEPD han venido adoptando cláusulas contractuales tipo[94], en relación a los distintos tipos de transferencias internacionales de datos[95].

En primer lugar, para las transferencias que se efectúen entre responsables del tratamiento cabe adoptar las cláusulas previstas en las Decisiones de la Comisión Europea 2001/497/CE, de 15 de junio de 2001, y 2004/915/CE, de 27 de diciembre de 2004, por la que se modifica la anterior[96]. En segundo lugar, para las transferencias internacionales de datos realizadas entre un responsable a un encargado del tratamiento deben utilizarse las cláusulas contractuales tipo fijadas en la Decisión de la Comisión Europea 2010/87/UE, de 5 de febrero de 2010. Por último, para las transferencias llevadas a cabo entre un encargado y un subencargado del tratamiento, debe acudirse a la resolución de la AEPD de Autorización de Transferencia Internacional de Datos de 16 de octubre de 2012, dónde se hallan las cláusulas tipo que aportan las garantías necesarias de protección de los datos personales de los titulares[97].

Sin embargo, a pesar de que se hayan adoptado las mencionadas cláusulas contractuales tipo, el Director o Directora de la AEPD puede denegar o suspender temporalmente la transferencia, *"previa audiencia del exportador de los datos*",

[94] Vid. Anexo del Trabajo.
[95] Vid. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Transferencias internacionales de datos*, Autorización de la Directora de la Agencia Española de Protección de Datos, en línea: https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides-idphp.php [consultado el 1.03.2016].
[96] "Cada una de las Decisiones de la Comisión Europea contiene un conjunto de cláusulas contractuales tipo. Los responsables del tratamiento podrán optar por uno u otro conjunto de cláusulas, pero no podrán modificarlas ni combinar elementos de distintas cláusulas ni de los conjuntos". AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Transferencias internacionales de datos*, Autorización de la Directora de la Agencia Española de Protección de Datos, en línea: https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides-idphp.php [consultado el 1.03.2016].
[97] "En el marco de protección de datos establecido por la Directiva 95/46/CE y en las Decisiones adoptadas por la Comisión Europea (…) se ha partido hasta la fecha de la configuración del exportador de datos como un responsable del tratamiento, sin que exista un modelo en la Unión Europea en que el exportador tenga la condición de encargado del tratamiento (…). Sin embargo, la inexistencia de un modelo de transferencia internacional de datos en el marco de la subcontratación de un encargado del tratamiento no implica que no sea dable a los Estados miembros la valoración de las garantías concurrentes en una transferencia de tal naturaleza". MARZO PORTERA, Ana; ORTEGA GIMÉNEZ, Alfonso, *Empresa y transferencia internacional de datos personales*, ICEX (Instituto Español de Comercio Exterior), Madrid, 2013, p. 42 y 43.

siempre que concurra alguna de las circunstancias enumeradas en el artículo 70.3 del Reglamento de la LOPD[98].

2.2.2. Normas corporativas vinculantes ("*Binding Corporate Rules*" o "BCR")

El uso de las normas corporativas vinculantes[99], como garantías adecuadas que pueden establecerse de forma alternativa a las cláusulas contractuales tipo, ha sido potenciado por el Grupo de trabajo del artículo 29 desde el año 2002[100]. En esencia, supone el establecimiento de las mismas normas o reglas internas en el seno de grupos multinacionales de empresas que garanticen el respeto del derecho fundamental a la protección de datos de los afectados y el cumplimiento de los principios y el ejercicio de los derechos reconocidos en la LOPD y su Reglamento.

Asimismo, su régimen jurídico se halla, por una parte, en los artículos 70.4 y el Título IX, Capítulo V del Reglamento de la LOPD y, por otra parte, en los Documentos de Trabajo elaborados por el Grupo del Artículo 29 de la Directiva 95/46/CE[101].

---

[98] "a) Que la situación de protección de los derechos fundamentales y libertades públicas en el país de destino o su legislación impidan garantizar el íntegro cumplimiento del contrato y el ejercicio por los afectados de los derechos que el contrato garantiza; b) Que la entidad destinataria haya incumplido previamente las garantías establecidas en cláusulas contractuales de este tipo; c) Que existan indicios racionales de que las garantías ofrecidas por el contrato no están siendo o no serán respetadas por el importador; d) Que existan indicios racionales de que los mecanismos de aplicación del contrato no son o no serán efectivos; y e) Que la transferencia, o su continuación, en caso de haberse iniciado, pudiera crear una situación de riesgo de daño efectivo a los afectados". Artículo 70.3 del Reglamento de la LOPD.

[99] Vid. Anexo del Trabajo

[100] "Su objetivo es flexibilizar los movimientos internacionales de datos personales a nivel global entre las sociedades pertenecientes a un mismo grupo multinacional de empresas que cuente con filiales establecidas tanto en países que ofrezcan un nivel de protección de los datos adecuado como en jurisdicciones que no garanticen el citado nivel". CÁRDENAS ARTOLA, Ignacio; FERRERO RECASENS, Eduardo, entre otros, ob.cit., p. 123.

[101] WP 155 – Preguntas más frecuentes sobre las BCRs, en línea: https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/common/wp155_en.pdf; WP 154 – Cuadro que establece la estructura de las BCRs, en línea: https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/common/wp154_en.pdf; WP 153 – Cuadro que establece la relación de los elementos y principios que deben contener las BCRs, en línea: https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/common/wp153_en.pdf; WP 108 – Modelo de solicitud de autorización de transferencia internacional basada en las BCRs en el ámbito del procedimiento coordinado, en línea: https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/common/wp108_en.pdf; WP 107 – Documento sobre la competencia de las Autoridades de Control europeas en el procedimiento coordinado de aprobación de las BCRs, en línea: https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/common/wp107_en.pdf; WP 74 – Documento sobre la aplicación del artículo 26.2 de la Directiva 95/46/CE a las BCRs, en línea: https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/common/wp74_en.pdf [consultado el 24.03.2016].

CAPÍTULO IV. LAS TRANSFERENCIAS INTERNACIONALES DE DATOS EN EL REGLAMENTO (UE) 2016/679 DEL PARLAMENTO Y DEL CONSEJO, DE 27 DE ABRIL DE 2016.

Tras cuatro años de trabajo, el día 14 de abril de 2016 el Parlamento Europeo adoptó el Proyecto de Reglamento general de protección de datos, tras haber manifestado su posición favorable el Consejo Europeo el pasado 8 de abril.

Con la pretensión de reformar de forma contundente la normativa comunitaria sobre protección de datos, adaptándola al contexto social y tecnológico actual, el Reglamento (UE) 2016/679 del Parlamento 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 ha derogado la Directiva 95/46/CE, cuya normativa ha sido la base fundamental del presente trabajo. No obstante, se observará que la esencia del régimen de las transferencias internacionales de datos no se ha visto modificada, sino que, por el contrario, se han positivizado ciertas prácticas que la Directiva 95/46/CE no regulaba, aumentándose con ello la seguridad jurídica en el flujo transnacional de datos.

En lo que al ámbito de aplicación temporal se refiere, el Reglamento entrará en vigor, al tenor su artículo 99, "*a los veinte días de su publicación oficial en el Diario Oficial de la Unión Europea*" y "*será aplicable a partir del 25 de mayo de 2018*", momento a partir del cual "*será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro*".

La regulación de las transferencias internacionales de datos la hallamos prevista en el Capítulo V del Reglamento general de protección de datos, cuyo principal objetivo sigue siendo el ponderar los dos intereses jurídicos en juego: por una parte no impedir los flujos transfronterizos de datos personales, que se estiman "*necesarios para la expansión del comercio y la cooperación internacionales*" y, por otra parte, la "*protección de las personas físicas*" en lo que a sus datos personales se refiere –si bien ahora ello se prevé en el Considerando 101, antes en Considerando 56 de la Directiva 95/46/CE.

A continuación se expondrán las principales novedades que la aprobación del nuevo Reglamento va a comportar en cuanto al régimen de las transferencias

internacionales de datos, destacando las diferencias más notables, y señalando aquello que se ha mantenido con respecto a las previsiones contenidas en la Directiva 95/46/CE.

En primer término, debe remarcarse que la nueva regulación de las transferencias internacionales de datos es mucho más detallada y precisa que los dos artículos de la antigua Directiva –los artículos 25 y 26-, dedicando ahora el Reglamento un total de 7 artículos a esta institución –desde el artículo 44 al artículo 50-. Como bien se apunta en el Considerando 101, ello se debe al aumento de los flujos transfronterizos de datos, lo cual plantea "*nuevos retos e inquietudes en lo que respecta a la protección de los datos de carácter personal*".

En segundo lugar, mientras que la Directiva 95/46/CE tan sólo atribuía la responsabilidad de cumplir con la normativa en relación con las transferencias internacionales de datos al responsable del tratamiento, ahora el Reglamento general de protección de datos también hace atribuye esta obligación al encargado del tratamiento.

Si bien en la Directiva 95/46/CE el punto de referencia que se establecía como destino de las transferencias era "el país tercero", ahora en el Reglamento se prevé que las mismas puedan realizarse también a organizaciones internacionales. Además, se especifica que el responsable y el encargado del tratamiento, deben cumplir con las condiciones establecidas en el Reglamento tanto con respecto a las transferencias internacionales de datos que ellos efectúen, como a las transferencias ulteriores que se hagan desde ese tercer país u organización internacional.

A los efectos de aumentar la "flexibilidad" en el ámbito de aplicación de las transferencias internacionales de datos, ahora las decisiones de adecuación de la Comisión Europea pueden referirse tanto a un *"tercer país*" u "*organización internacional*", como a un "*territorio*" o a "*uno o varios sectores específicos de ese tercer país*". Como ya sucedía en la regulación de la Directiva 95/46/CE, las transferencias que se realicen al país, organización internacional, territorio o sector de ese tercer país que gozan nivel de protección adecuado declarado por una decisión de adecuación de la Comisión no necesitan ninguna autorización específica.

En quinto lugar, conviene subrayar que el artículo 45.2 del Reglamento ha incrementado los criterios a los que debe atenerse la Comisión para emitir la decisión de

adecuación[102]. Deseo remarcar la adición del criterio de atender a "*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 valoración de "*la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos*".

Conviene destacar que la Comisión puede emitir su decisión de adecuación mediante un "acto de ejecución", debiendo establecer un mecanismo de revisión periódica, al menos cada cuatro años, "*que tenga en cuenta todos los acontecimientos relevantes en el tercer país o en la organización internacional*".

De suma importancia es el aumento de la tipificación legal de lo que se estiman "garantías adecuadas". Ahora el artículo 46 del Reglamento señala que, a falta de una decisión de adecuación por parte de la Comisión, las transferencias internacionales de datos podrán realizarse si se cumplen dos condiciones: por una parte, si el responsable o el encargado del tratamiento ha "*ofrecido garantías adecuadas*" y, por otra parte, se establece la condición de que "*los interesados cuenten con derechos exigibles y acciones legales efectivas*".

Así mismo, se prevén dos tipos de "garantías adecuadas", pues las detalladas en el apartado 2 del artículo 46 no requieren ninguna autorización expresa de una autoridad de control, y las previstas en el apartado 3 del mismo artículo sí que hacen necesaria

[102] De acuerdo con el artículo 45.2 del Reglamento, "Al evaluar la adecuación del nivel de protección, la Comisión tendrá en cuenta, en particular, los siguientes elementos: a) 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 recursos administrativos y acciones judiciales que sean efectivos; b) la existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros, y c) los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales".

dicha autorización. En cuanto a las primeras, el Reglamento añade las normas corporativas vinculantes, los instrumentos jurídicamente vinculantes y exigibles entre las autoridades u organismos públicos, así como los mecanismos de certificación aprobados con arreglo al artículo 42, "*junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados*". En particular, el Reglamento dedica el artículo 47 a regular la el mecanismo de las normas corporativas vinculantes, detallando sus requisitos y el contenido mínimo que deben incluir.

En cuanto a las garantías que requieren de la correspondiente autorización, se prevén las "*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*" y las "*disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados*".

Por último, deseo señalar que el artículo 49 del Reglamento, como ya realizaba el artículo 26 de la Directiva 95/46/CE, establece un conjunto de "*excepciones para situaciones específicas*", situaciones tasadas en que, en ausencia de decisión de adecuación o de garantías adecuadas, pueden efectuarse igualmente transferencias internacionales de datos personales a un tercer país u organización internacional. Esencialmente se mantienen las excepciones que ya preveía la Directiva 95/46/CE, aunque se añaden ciertas particularidades.

A título ilustrativo, conviene apuntar que ahora, el consentimiento que efectúe el interesado a la transferencia propuesta debe aportarse "*tras haber sido informado de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas*"; también, la excepción de cuando "*la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento y un tercero*" prevista en el artículo 26.1 c) de la Directiva, el Reglamento ha suprimido la adición de "*o por celebrar en interés del interesado"*. Por último, en cuanto a la excepción del artículo 26.1 c) de la Directiva, que decía cuando "la transferencia sea necesaria para la salvaguardia del interés vital del interesado", ahora el Reglamento ha añadido la protección de los intereses vitales "*de otras personas*".

Finalmente, resulta sorprendente la "excepción de la excepción" que establece el Reglamento en el último párrafo del artículo 49.1. Al tenor de la misma, cuando una transferencia no se base en una decisión de adecuación ni aporte garantías adecuadas y no sea aplicable ninguna de las excepciones para situaciones específicas del artículo 49.1 del Reglamento, "*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*". En estos casos, el responsable del tratamiento debe informar a la autoridad de control y al interesado de la transferencia en cuestión, y de los intereses legítimos imperiosos perseguidos.

CAPÍTULO V

LAS TRANSFERENCIAS INTERNACIONALES DE DATOS CON DESTINO A ESTADOS UNIDOS DE AMÉRICA

I. LA PROTECCIÓN JURÍDICA DE LOS DATOS PERSONALES EN ESTADOS UNIDOS DE AMÉRICA.

1. Instrumentos normativos que protegen los datos personales en Estados Unidos de América.

Como se señala en el Preámbulo de los Principios de Puerto Seguro, aunque EE.UU y la UE comparten el objetivo de mejorar la protección de la vida privada de sus ciudadanos, sus métodos varían sustancialmente, pues el planteamiento de EE.UU es de carácter sectorial, presentando como fundamento una mezcla de legislación, reglamentación y autorregulación.

Conviene destacar que, de acuerdo con el Parlamento Europeo, la Directiva 95/46/CE exige que la persona interesada goce de derechos específicos cuando se

efectúe un tratamiento de sus datos personales[103]. No obstante, del análisis de la protección estadounidense de los datos, el Parlamento apuntó que "*quedará de manifiesto la preocupación del Parlamento por la inexistencia del derecho personal de reclamación judicial, así como por la falta de acuerdo para obligar a las empresas a indemnizar por la utilización ilegal de datos*".

Como Estado Federal, EE.UU se halla integrado por 50 Estados y el Distrito de Colombia[104] y dentro de la distribución de competencias entre Federación y Estados federados, la "*privacy"* es una de las materias "concurrentes" que pueden hallarse reguladas tanto por la Federación como por los Estados miembros.

Conviene remarcar que, en el ámbito internacional EE.UU, ha ratificado las Directrices sobre protección de la vida privada de la OCDE de 1980 y reafirmaron su aplicabilidad, con especial referencia al *e-commerce*, en 1998[105].

En cuanto al ámbito interno, es necesario recalcar que en EE.UU la protección de la "*privacy*" difiere en el ámbito público y privado. Si atendemos a su reconocimiento constitucional en la Quinta[106] y, especialmente, la Cuarta Enmienda de la *Constitution of the United States of America*, las mismas presentan como destinatario únicamente al sector público, sin que obliguen al sector privado, según la *US Suprem Court*[107]. La Cuarta Enmienda de la *Constitution of the United States of America*, recoge el derecho del individuo a la seguridad de su persona, de sus domicilios, papeles y efectos, contra

[103] Vid. Resolución del Parlamento Europeo sobre el proyecto de decisión de la Comisión relativa a la adecuación de la protección garantizada por los principios estadounidenses de puerto seguro y preguntas más frecuentes relacionadas publicadas por el Departamento de Comercio de los EE.UU. (C5-0280/2000 – 2000/2144 COS), Considerando d) y apartado 13 de la Resolución.

[104] Vid. UNITED STATES CENSUS BUREAU: U.S. and World Population Clock, en línea: http://www.census.gov/popclock/ [consultado el 4.04.2016].

[105] Vid. ARRIBAS LUQUE, José María, "Sobre la protección adecuada en las transmisiones de datos personales desde la Unión Europea a los EE.UU.: El sistema de principios de Puerto Seguro", *Diario La Ley*, nº 549, (2002), p. 2.

[106] No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation. THE FIFTH AMENDMENT: Rights of persons, en línea: https://www.congress.gov/content/conan/pdf/GPO-CONAN-REV-2014-10-6.pdf [consultado el 16.03.2016].

[107] "Así, mientras que la obligación del sector público ha de regularse mediante leyes, a los particulares no se les puede imponer una obligación que no deriva de la Constitución y que coartaría directamente el derecho constitucional consagrado en la Primera Enmienda (…).Y a esta imposibilidad de obligación forzosa hay que unir el que la industria norteamericana se opuso tradicionalmente a la voluntaria limitación de su derecho al uso de datos personales, en su propio beneficio y como herramienta commercial" ARRIBAS LUQUE, José María, ob. cit., p. 2 y 3.

registros e incautaciones irrazonables[108]. Así mismo, se hallan protegidos bajo la Cuarta Enmienda tanto los actos del Gobierno obteniendo información mediante su acceso físico en un área constitucionalmente protegida, así como cuando viola una expectativa de privacidad que la sociedad reconoce como razonable[109].

En el ámbito privado, la industria norteamericana se opuso tradicionalmente a la limitación de su derecho al uso de los datos personales, en su propio beneficio y como herramienta comercial. Pese a ello, apunta ARRIBAS LUQUE, "la irrupción de las nuevas tecnologías y la escasa protección legislativa de la *privacy* motivó la pérdida de la confianza del consumidor norteamericano y ello forzó la autoimposición empresarial, voluntaria y como táctica comercial, como normas de conducta limitativas del libre uso de los datos personales". De este modo, la protección de los datos personales en EE.UU en el ámbito privado se vino confeccionando mediante la autorregulación o *self-regulation* de los propios sectores o empresas, y no como obligación impuesta por el Estado.

No obstante lo expuesto con anterioridad, cabe remarcar la existencia en EE.UU de acciones judiciales que, a pesar de no ser específicas, pueden proteger los datos personales.

En primer lugar, el *Second Restatement of the Law Torts*[110] del *American Law Institute* establece acciones de "responsabilidad por falsa declaración" para el caso que

[108] FOURTH AMENDMENT: The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated; and no Warrants shall issue but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. THE FOURTH AMENDMENT: Search and seizure, en línea: https://www.congress.gov/content/conan/pdf/GPO-CONAN-REV-2014-10-5.pdf [consultado el 16.03.2016].

[109] Vid. J. SOLOVE, Daniel, "A Brief History of Information Privacy Law", en DANIEL J. SOLOVE, MARC ROTENBERG Y PAUL M. SCHWARTZ, *Information Privacy Law*, Ed. Wolters Kluwer, New York, 2006, p. 22.

[110] En primer lugar, de acuerdo con FURNISH los *Restatements of the Law* son una fuente positiva y concreta del Derecho estadounidense, que se hallan elaborados en el marco del *American Law Institute*, como institución dotada de juristas de reputado prestigio influentes en el ámbito del Derecho. Como expone el autor, "lo elaboraron los mismos jueces que lo aplicaban junto con los mismos abogados que lo alegaban y los mismos académicos que lo comentaban". No obstante su evidente autoridad normativa, apenas se examinará la jerarquía exacta de esta norma. El autor propone al lector una definición de los *Restatements of the Law*, como "declaración de reformulación escrita, completa, lógica y sistemática de todo el derecho en vigencia para la jurisdicción que lo aplicará, en derogación de las normas anteriores. Son compresivos, basados en la experiencia, deben contener principios generales, no entran en vigencia formal por la aprobación y promulgación del poder legislativo, pero sí se aplican por los tribunales". En los que a sus objetivos se refiere, los *Restatements of the Law* se hallan formulados de manera similar al Código Civil, al igual que juegan un papel muy parecido a éste. De este modo, declaran y recogen

alguna entidad norteamericana incumpla sus políticas de privacidad, apuntando que "quien realice fraudulentamente una falsa declaración de hechos, opiniones, intenciones o normas jurídicas con el fin de inducir a otro a actuar o abstenerse de actuar por tal motivo, será responsable frente a quien ha sido objeto del engaño de las pérdidas económicas que éste hubiera sufrido por haberse basado justificadamente en tal falsa declaración".

En segundo lugar, cabe señalar las acciones que prevé el *common law* norteamericano para reclamar indemnizaciones por daños y perjuicios por violación del derecho a la intimidad. Estas acciones provienen de normas impuestas por los Tribunales a través del precedente vinculante o *binding precedent*, como esencia del Derecho anglosajón del *case law*, en que los Tribunales se hallan obligados de aplicar lo que se decidió y aplicó en casos similares tribunales jerárquicamente superiores[111].

Por último cabe destacar las medidas de protección de la *privacy* impuestas por diversas leyes federales y estatales, que establecen indemnizaciones por los daños y perjuicios sufridos por los particulares por haberse vulnerado su derecho a la privacidad[112]. A título ilustrativo cabe citar la *Electronic Communications Privacy Act* de 1986, la *Telecommunications Act* de 1996 y la *Consumer Credit Reporting Reform Act* de 1996.

2. Evolución de los mecanismos de protección de los datos personales en Estados Unidos de América.

En Estados Unidos, el desarrollo más profundo del derecho a la privacidad se llevó a cabo mediante la publicación en la *Harvard Law Review* el 1890 del artículo "*The Right to Privacy*", de SAMUEL D. WARREN Y LOUIS D. BRANDEIS[113], que destacó la

principios del Derecho americano, concretamente del derecho civil americano. Así pues, la existencia de un cuerpo normativo a nivel "americano", como lo es los *Restatements of the Law*, es algo realmente singular, teniendo en cuenta que en EE.UU cada Estado regula su propio Derecho, sin perjuicio de la normativa especial en lo referente a cuestiones federales. FURNISH, Dale Beck, *Fuentes del Derecho en Estados Unidos. La muerte del derecho consuetudinario. Las fuentes escritas en la edad del derecho positivo, y el papel y efecto de los Restatements of the law,* en línea: http://www.juridicas.unam.mx/publica/librev/rev/facdermx/cont/235/art/art3.pdf [consultado 10.12.2015].

[111] Vid. ARRIBAS LUQUE, José María, ob. cit., p. 6.

[112] Vid. ARRIBAS LUQUE, José María, ob. cit., p. 5.

[113] "The piece reflected on the harms caused by gossip and press intrusions into people's private lives, and argued that judges could (and should) make use of existing legal authority to recognize a new tort for the

necesidad de proteger "*the more general right of the individual to be let alone*"[114]. Posteriormente, en 1960, WILLIAM PROSSER analizó los trecientos casos creados por Warren y Brandeis, y concluyó que podían agruparse en cuatro categorías distintas de agravios o ataques al derecho a la privacidad: en primer término, los casos de "*instrusion upon seclusion*" o intrusión en la intimidad; en segundo lugar, de "*public disclosure of private facts*" o publicación de hechos privados; en tercer lugar, de "*false light or publicity*" o publicidad denigratoria y, por último, la "*appropriation*" o apropiación del nombre o apariencia de otro en beneficio propio.

Con posterioridad, se confeccionó el derecho a la *informational privacy,* como la capacidad que tienen los individuos de controlar la información, que sobre ellos mismos, se comunica a terceros, cuya primera plasmación la hallamos en la *Fair Credit Reporting Act*, de 26 de octubre de 1970.

Poco después de que el invento del teléfono fuese patentado en 1976 se desarrollaron los métodos para interceptar las comunicaciones efectuadas mediante este instrumento. Ahora bien, en 1928 la Corte Suprema de EE.UU en el caso *Olmstead v. United States* apuntó que la Cuarta Enmienda no se aplicaba a las interceptaciones telefónicas porque ello no implicaba intrusión en el hogar[115].

Seis años después del caso *Olmstead*, el Congreso promulgó la Sección 605 de la *Federal Communications Act* de 1934, declarando que "*ninguna persona sin la correspondiente autorización por el remitente puede interceptar ninguna comunicación y divulgar, publicar o comunicar a ninguna persona la existencia, el contenido, las intenciones, el efecto o el significado de estas comunicaciones interceptadas*"[116].

No obstante, esta norma únicamente se aplicaba a los oficiales federales, no de carácter estatal, y realmente no les prohibía efectuar intervenciones en la línea telefónica, sino tan sólo el revelar esta información obtenida de comunicaciones interceptadas. En consecuencia, las intervenciones telefónicas efectuadas por el FBI y los oficiales estatales a lo largo del siglo XX aumentaron dramáticamente, a lo cual

---

invasion of individual privacy". HARVARD LAW REVIEW, commentary by Charles E. Colman, en línea: http://harvardlawreview.org/2016/01/about-ned/ [consultado el 25.03.2016].

[114] Vid. J. SOLOVE, Daniel, "A Brief History of Information Privacy Law", en DANIEL J. SOLOVE, MARC ROTENBERG Y PAUL M. SCHWARTZ, *Information Privacy Law*, Ed. Wolters Kluwer, New York, 2006, p. 12.

[115] Vid. J. SOLOVE, Daniel, ob. cit., p. 18.

[116] Vid. J SLOVE, Daniel, ob.cit., p. 19.

deberá añadirse la revolución ocasionada por el surgimiento del ordenador[117], en lo que a la manera recoger y usar los datos de carácter personal se refiere.

En 1968 el Congreso amplió la protección legal contra la vigilancia electrónica, más allá de la limitada protección que otorgaba la sección 605. El Título III de la *Omnibus Crime Control and Safe Streets Act* extendió el alcance de la regulación de las intervenciones telefónicas a los oficiales estatales, así como a los sujetos privados. Sin embargo, dicho Título III no se aplicaba a las vigilancias de carácter visual, y tampoco a otras formas de comunicaciones electrónicas.

A ello debe agregarse la aprobación en 1978 de la *Foreign Intelligence Surveillance Act* o "FISA", que creó una regulación distinta de la vigilancia electrónica destinada a recoger información de inteligencia extranjera, reduciendo la protección contra la vigilancia electrónica prevista en la Cuarta Enmienda.

A finales de la década de 1970 la Corte Suprema tomó varias decisiones reduciendo el alcance de la protección contenida en la Cuarta Enmienda. Por ejemplo, en 1979 la Corte concluyó, en el caso *Smith v. Maryland* que la Cuarta Enmienda no era aplicable a la lista de números de teléfono que una persona marca, que se hallan grabados en el registro de llamadas. De acuerdo con la Corte, "desde el momento en que la gente sabe que ellos deben transmitir información respecto tales número de teléfono a la compañía telefónica, no pueden tener ninguna expectativa de que tales números permanecerán secretos"[118].

El 1986 se promulgó la *Electronic Communications Privacy Act,* que expandió el Título III de la *Omnibus Crime and Control Act* de 1968 –estatuto creado para regular la vigilancia electrónica para investigaciones criminales en el ámbito de Estados Unidos- a nuevos medios de comunicación, prestando una especial atención al ámbito de los ordenadores. El ECPA restringió la intercepción de comunicaciones transmitidas y la búsqueda de comunicaciones y archivos guardados por los proveedores de servicios de comunicaciones, así como reguló los límites de los registros de llamadas.

[117]"Internet is the most fruitful área for data collection in modern times. It is quite posible to collect tremendous amunts of data on almost all users od the internet without their knowledge". HOLVAST, Jan, "History of Privacy", ob. cit., p. 24.

[118] Vid. J SLOVE, Daniel, ob. cit., p. 31.

Poco después de los ataques terroristas acaecidos el 11 de septiembre de 2001, en Estados Unidos hubo un fuerte impulso político para instaurar nuevas medidas de vigilancia y nuevos poderes de las fuerzas del orden. Con este propósito el Congreso Promulgó el "*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*" (en adelante "USA PATRIOT Act")[119], que llevó a cabo profundos cambios en la ECPA y la FISA, entre otras normas. Posteriormente, en 2004 el Congreso promulgó *"The Intelligence Reform and Terrorism Prevention Act"* para facilitar la comunicación de información entre las agencias federales.

Por último, conviene destacar la reforma de la FISA en 2008, que fue aprobada por el Senado de EE.UU con 69 votos a favor y 28 en contra, cuya pretensión era "saber lo que dicen (los terroristas) y lo que están planeando". Entre otros elementos, la iniciativa autorizó las escuchas sin necesidad de permiso judicial a quienes utilizasen las redes de EE.UU, sean estadounidenses o de extranjero, así como actualizar la FISA de 1978 a las innovaciones tecnológicas como Internet y los teléfonos móviles[120].

II. ANÁLISIS CRÍTICO DE LA DECISIÓN DE LA COMISIÓN EUROPEA DE 26 DE JULIO DE 2000 SOBRE LA ADECUACIÓN CONFERIDA POR LOS PRINCIPIOS DE PUERTO SEGURO PARA LA PROTECCIÓN DE LA VIDA PRIVAYA Y LAS CORRESPONDIENTES PREGUNTAS MÁS FRECUENTES.

En virtud del artículo 25.6 de la Directiva 95/46/CE, la Comisión Europea puede hacer constar que un país tercero garantiza un nivel de protección adecuado a los efectos de protección de la vida privada o de las libertades y los derechos fundamentales de las personas, momento a partir del cual pueden efectuarse transferencias internacionales de datos "sin que sea necesaria ninguna garantía adicional"[121]. Por ello, el estimar si el

[119] Vid. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, en línea: https://www.congress.gov/bill/107th-congress/house-bill/3162 [consultado el 15.04.2016].

[120] Vid. EL MUNDO, El Senado de EEUU aprueba la nueva Ley de Escuchas Telefónicas, 10 de julio de 2008, en línea: http://www.elmundo.es/elmundo/2008/07/10/internacional/1215647473.html [consultado el 15.04.2016].

[121] Vid. Considerando número 2 de la Decisión de la Comisión de 26 de Julio de 2000, con arreglo a la Directiva 95/46/CE, sobre la adecuación conferida por los principios de puerto seguro para la protección

contenido de los Principios de Puerto Seguro y sus correspondientes Preguntas más Frecuentes aportan o no un nivel adecuado de protección de los datos personales resulta esencial.

Mediante su Decisión de 26 de Julio de 2000, la Comisión Europea condicionó el nivel adecuado de protección de la transferencia internacional de datos efectuada desde la Unión Europea a Estados Unidos de América al cumplimiento por las entidades de los Principios de Puerto Seguro o *Safe Harbor Privacy Principles* y de las correspondientes Preguntas más Frecuentes o *Frequently Asked Questions* (en adelante, "FAQ"), como criterios de orientación para la correcta aplicación de los principios en cuestión, todo ello publicado el 21 de julio del 2000 por el *US Department of Commerce.*

En esencia, la Decisión se halla estructurada en cinco partes fundamentales. En primer lugar, tras exponer sus once considerandos, se recoge la decisión *strictu sensu*, que se halla compuesta de 6 artículos; en segundo lugar, el Anexo I formula los "Principios de puerto seguro (Protección de la vida privada)" y, en tercer lugar, el Anexo II detalla quince FAQ. Posteriormente, los Anexos III a VII prescriben un conjunto de criterios y resuelven dudas acerca la aplicación de los principios de puerto seguro y las FAQ[122].

Ya en la Opinión 1/99 el Grupo de Trabajo del Artículo 29 (en adelante, "GT29") solicitó a los EE.UU. la aclaración del estatus o la naturaleza de los principios[123], así como de las preguntas más frecuentes. Con respecto a esta cuestión, en el documento de trabajo del GT29 de 7 de julio de 1999 se afirmó que las preguntas más frecuentes debían ser una parte integral y esencial del acuerdo de Puerto Seguro, gozando de la

---

de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de los Estados Unidos de América.

[122] En el Anexo III figura un Estudio de Aplicación; en el Anexo IV se recoge un Memorando sobre daños y perjuicios por violación de la vida privada y autorizaciones explícitas en la legislación estadounidense; en el Anexo V se encuentra una Carta de la Comisión Federal de Comercio y en el Anexo VI una Carta del Departamento estadounidense de Transporte.

[123] "Generally, the status of these principles needs to be clarified. Whilst adherence to the principles in the first instance can be voluntary, once a company does decide to adhere and thereby to claim the benefit of "safe harbor", compliance must be compulsory". Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Comission and the United States Government, adopted by the Working Party on 26 January 1999 (5092/98/EN/final WP 15), p. 3.

misma fuerza vinculante que los Principios[124]. Por ello, el GT29 estima que, a los efectos de valorar el nivel de protección adecuado, el enfoque debe ser global.

Al tenor del artículo 1.2 de la Decisión, en relación con cada transferencia de datos deberán cumplirse las condiciones siguientes: por una parte "*la entidad receptora de los datos deberá haber manifestado de forma inequívoca y pública su compromiso de cumplir los principios aplicados de conformidad con las FAQ*"; por otra parte, *"la entidad estará sujeta a la jurisdicción de uno de los organismos públicos estadounidenses que figuran en el anexo VII de la presente Decisión, que estará facultado para investigar las quejas que se presenten y solicitar medidas provisionales contra las prácticas desleales o fraudulentas, así como reparaciones para los particulares, independientemente de su país de residencia o de su nacionalidad, en caso de incumplimiento de los principios y su aplicación de conformidad con las FAQ*".

A continuación se procederá a efectuar un análisis crítico de la protección conferida por los Principios y las FAQ, para lo cual se atenderá a las opiniones y a los documentos emitidos por el Grupo de Trabajo del Artículo 29 y por la Comisión.

1. Elementos de carácter formal.

1.1. La inadecuación del artículo 1 de la Decisión al artículo 25 apartado 6 de la Directiva 95/46/CE.

Al tenor literal del artículo 25 apartado 6 de la Directiva 95/46/CE la Comisión puede hacer constar "*que un país tercero garantiza un nivel de protección adecuado (...) a la vista de su legislación interna o de sus compromisos internacionales (...) a efectos de protección de la vida privada o de las libertades o de los derechos fundamentales de las personas*". Por lo tanto, la primera objeción que cabe realizar a los Principios y a las FAQ es que los mismos no aseguran que los Estados Unidos de América, como país tercero, garantice un nivel de protección adecuado "*a la vista de su legislación interna o de sus compromisos internacionales, (...) a efectos de protección*

[124] "Since having been informed by the Commission that the FAQs are to be an integral part of the Safe Harbor arrangement and to have the same binding force as the Principles, the Working Party considers that henceforth its approach has to be comprehensive with regard to both texts and it should therefore issue an opinion covering both the Principles and the FAQs. It follows that until the Working Party has all the FAQs announced by the American side as well as the related legal texts it will not be able to deliver a complete and definitive opinion on the "Safe Harbor arrangement". Working Document on Functioning of the Safe Harbor Agreement, adopted on 2 July 2002 (11194/02/EN WP 62), p. 2.

de la vida privada o de las libertades o de los derechos fundamentales de las personas"[125].

Si atendemos a la "*legislación interna o los compromisos internacionales"* de EE.UU, ya el GT29 señaló en su Opinión 1/99, de 26 de enero de 1999 que "la privacidad y la protección de los datos personales en Estados Unidos se hallan reguladas bajo una compleja normativa sectorial, tanto a nivel federal como estatal, a lo cual se añade la autorregulación propia de cada sector". Por ello, "a pesar de los esfuerzos que se han llevado a cabo para mejorar la credibilidad y aplicabilidad de la autorregulación sectorial", el GT29 apuntó que "el actual mosaico de normas sectoriales no puede (…) ser invocado para proporcionar una protección adecuada para los datos personales transferidos desde la Unión Europea"[126].

Por lo tanto, el nivel adecuado de protección de los datos personales en el ordenamiento jurídico norteamericano, conferido al tenor de la Decisión, depende principalmente del contenido y la efectiva aplicación de los Principios de Puerto Seguro y las FAQ, y no de la "*legislación interna o los compromisos internacionales"* del país tercero, EE.UU.

1.2. El sistema de adhesión a los Principios de Puerto Seguro y a sus correspondientes Preguntas más Frecuentes y sus límites.

En segundo lugar, cabe subrayar que la decisión de adherirse a los requisitos de "Puerto Seguro" por parte de las entidades norteamericanas, además de ser totalmente voluntaria[127], se realiza conforme a un sistema de auto-certificación[128], en que la entidad de forma autónoma valora que reúne las condiciones mencionadas en los Principios y las FAQ, y posteriormente notifica al Departamento de Comercio de Estados Unidos de América o a su representante su compromiso con respecto a dicho cumplimiento. De

[125] Vid. Artículo 25.6 de la Directiva 95/46/CE.

[126] Vid. Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Comission and the United States Government, adopted by the Working Party on 26 January 1999 (5092/98/EN/final WP 15) y Opinion 2/99 on the Adequacy of the "International Safe Harbor Principles" isued by the US Department of Commerce on 19th April 1999, adopte don 2 May 1999 (5047/99/EN/final WP 19).

[127] Como apunta ARRIBAS LUQUE, el sistema de protección no podía tener, por imposibilidad política más que jurídica, un enfoque legislativo, decantándose el US Department of Commerce por la fórmula de proponer a las entidades norteamericanas un código de principios al que podrían acogerse libre y voluntariamente. Vid. ARRIBAS LUQUE, ob. cit., p. 7.

[128] De acuerdo con la FAQ número 6, "los beneficios del puerto seguro se garantizan desde la fecha en que una entidad autocertifica ante el Departamento de Comercio, o su representante, su adhesión a los principios de conformidad con las directrices que se indican a continuación".

ello se infiere que, como bien señala el GT29 en su Opinión 7/99, "no existe control previo por parte del Departamento de Comercio con el fin de determinar si una entidad en concreto cumple con los Principios y las FAQ"[129] en su política de privacidad.

Sin embargo, conviene remarcar que, desde 2009 y como respuesta a las peticiones de la Comisión, el Departamento de Comercio ha venido efectuando un control "formal" de las nuevas solicitudes de adhesión al acuerdo de Puerto Seguro, sin que se evaluasen las prácticas reales. A título meramente ilustrativo cabe mencionar que el número de solicitantes que no superaron el examen administrativo del Departamento de Comercio y, por tanto, no fueron incluidos en la lista de puerto seguro en 2010 fue tan sólo un 6 % de las 513 y en 2013 un 12% de las 605 entidades que lo solicitaron[130].

A ello se añade las excepciones previstas en el cuarto párrafo de los Principios, según el cual la adhesión a los mismos puede limitarse "*cuando sea necesario para cumplir las exigencias de seguridad nacional, interés público y cumplimiento de la ley", y "por disposición legal o reglamentaria, o jurisprudencia que originen conflictos de obligaciones o autorizaciones explícitas".*

El GT29 ha venido reiterando su preocupación con respecto a la facultad de que gozan las autoridades estadounidenses de establecer excepciones a los Principios a través de la regulación, "sin dar la debida importancia a los intereses de protección de la privacidad"[131]. En este sentido, el GT29 señala en su Opinión 7/99 la necesidad de establecer una clara distinción entre las "opciones" y las "obligaciones": "*adherence to the principles should only be limited to the extent necessary to comply with statutory or regulatory obligations (which would in any case override the principles) but not as a result of options which may result from US law, as this would result in a serious weakening of the principle*"[132].

---

[129] Vid. Opinion 7/99 on the Level of Data Protection provided by the "Safe Harbor" Principles as published together with the Frequently Asked Questions (FAQs) and other related documents on 15 and 116 November 1999 by the US Department of Commerce, adopted on 3 December 1999 (5146/99/EN/final WP 27).

[130] Vid. Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE, de 27 de noviembre de 2013, COM (2013) 847 final, p. 10.

[131] Vid. Working documento n the current state of play of the ongoing discussions between the European Comission and the United States Government concerning the "International Safe Harbor Principles", adopte don 7 July 1999 (5075/99/EN/final WP 23).

[132] Vid. Opinion 7/99 on the Level of Data Protection provided by the "Safe Harbor" Principles as published together with the Frequently Asked Questions (FAQs) and other related documents on 15 and

2. Elementos de carácter material.

2.1. La ambigüedad del ámbito de aplicación de la Decisión de la Comisión de 26 de julio de 2000 y las competencias limitadas de los organismos públicos enumerados en el anexo VII de la Decisión.

La tercera crítica que cabe realizar a la Decisión de la Comisión, es el ambiguo ámbito de aplicación de los Principios de Puerto Seguro y de las FAQ, previsto en el artículo 1.1 de la Decisión[133]. En particular, ya recomendó el GT29 en su Opinión 7/99 que el ámbito de aplicación se definiera de forma más clara y sin ambigüedad con respecto a los beneficiarios y a las categorías de transferencias de datos[134].

Por una parte, los Principios son aplicables únicamente a las entidades estadounidenses autocertificadas que reciban datos personales desde la UE, sin que se exija a las autoridades públicas estadounidenses su sumisión estos principios[135].

Dado que la eficacia del régimen de Puerto Seguro depende directamente de la sumisión de las entidades adheridas al mismo a la jurisdicción de los organismos previstos en el Anexo VII de la Decisión –la FTC o el Departamento de Transporte-, los sectores que se hallan excluidos de la jurisdicción de dichos organismos públicos limitan el ámbito de aplicación de dicho régimen.

Si una entidad autocertificada incumple sus políticas de privacidad, según la literalidad del párrafo tercero del Anexo I de la Decisión, dicho incumplimiento "*se*

---

116 November 1999 by the US Department of Commerce, adopted on 3 December 1999 (5146/99/EN/final WP 27), p. 5.

133 "A los efectos del apartado 2 del artículo 25 de la Directiva 95/46/CE, para todas las actividades cubiertas por la misma, se considerará que los principios de puerto seguro, (en lo sucesivo denominados «los principios»), que figuran en el anexo I de la presente Decisión, aplicados de conformidad con la orientación que proporcionan las preguntas más frecuentes (en lo sucesivo denominadas «FAQ») publicadas por el Departamento de Comercio de Estados Unidos de América con fecha 21 de julio de 2000, que figuran en el anexo II de la presente Decisión, garantizan un nivel adecuado de protección de los datos personales transferidos desde la Comunidad a entidades establecidas en Estados Unidos de América". Artículo 1.1 de la Decisión de la Comisión de 26 de julio de 2000.

134 "As regards the "Safe Harbor", the Working Party recommends that its scope be clearly and unambiguously defined with regard to both the beneficiaries and the categories of data transfers": Opinion 7/99 on the Level of Data Protection provided by the "Safe Harbor" Principles as published together with the Frequently Asked Questions (FAQs) and other related documents on 15 and 116 November 1999 by the US Department of Commerce, adopted on 3 December 1999 (5146/99/EN/final WP 27), p. 3.

135 "Las entidades sujetas a disposiciones de naturaleza legal, reglamentaria, administrativa u otra (o a reglamentaciones), que protejan con eficacia el secreto de los datos personales, podrán acogerse también a los beneficios del puerto seguro". Párrafo tercero del Anexo I de la Decisión de la Comisión de 26 de julio de 2000.

persigue en virtud del artículo 5 de la Federal Trade Commission Act por la que se prohíben las prácticas desleales o fraudulentas, o de otras leyes o normativas similares". En este punto, cabe apuntar la falta de concreción y la inexactitud con la que se regulan los supuestos de vulneración de las políticas de privacidad, pues no se establece de forma precisa la normativa estadounidense que persigue el incumplimiento de las políticas de privacidad de las entidades adheridas al régimen de Puerto Seguro.

Prosiguiendo con el análisis, las empresas adheridas a los beneficios del Puerto Seguro se encuentran sujetas a la jurisdicción de como mínimo uno de los organismos públicos enumerados en el anexo VII de la presente Decisión, que son la *Federal Trade Commission* y el Departamento de Transporte de Estados Unidos de América.

La primera actúa en el ejercicio de la competencia que le confiere el artículo 5 de la *Federal Trade Commission Act*, actuando contra los actos desleales y engañosos que tengan lugar en el "ámbito del comercio", y no aquéllos datos procesados sin finalidad comercial –como por ejemplo, aquéllos que se utilicen sin fines de lucro o para investigación-.

Dada la inseguridad jurídica que ello comporta, el GT29 en sus documentos de trabajo de 7 de julio y de 3 de diciembre de 1999, ya solicitó aclaraciones sobre dos puntos específicos: por una parte, de los sectores que se hallarían excluidos del ámbito de aplicación de los Principios de Puerto Seguro, ya que no caen dentro de la jurisdicción de un organismo público similar a la FTC, y por otra parte, de las actividades que una entidad adherida al Puerto Seguro puede excluir de su política de privacidad, por estimar que no se halla comprendida en el ámbito de aplicación de los mismos[136].

Es más, el mismo Anexo VII de la Decisión detalla que la FTC carece de jurisdicción "*en lo tocante a bancos, cooperativas de ahorro y crédito, compañías de*

[136] En la Opinipin 7/99 el GT29 señala: the Working Party notes that FAQ 6 invites organisations to indicate the "activities of the organisation covered by its "Safe Harbor" commitments". This implies that the same organisation could enter the "Safe Harbor" with one foot and keep the other foot out of the "Safe Harbor". The Working Party takes the view that this creates legal uncertainty (in particular with regard to data sharing within an organisation) and urges clarification on the notion of "activities". Opinion 7/99 on the Level of Data Protection provided by the "Safe Harbor" Principles as published together with the Frequently Asked Questions (FAQs) and other related documents on 15 and 116 November 1999 by the US Department of Commerce, adopted on 3 December 1999 (5146/99/EN/final WP 27), p. 7.

servicio público de telecomunicaciones y de transporte, compañías aéreas y envasadores y operarios de áreas para ganado"[137].

Por otro lado, el Departamento de Transporte de Estados Unidos de América actúa en el ejercicio de su competencia, que le confiere la sección 41712 del título 49 del *United States Code* incoando los procedimientos basándose tanto en sus propias investigaciones como en las acusaciones formales e informales recibidas de particulares, agentes de viajes, compañías aéreas, organismos públicos estadounidenses y extranjeros.

Conforme a la FAQ número 11, denominada "Resolución de litigios y ejecución", existen dos mecanismos de resolución de quejas por vulneración de los Principios de Puerto Seguro. En primer término, cabe acudir al mecanismo de Resolución Alternativa de Conflictos (*Alternative Dispute Resolution* o ADR)[138], los cuales pueden presentar los casos a la FTC y, por otra parte, el particular puede presentar sus quejas directamente a la FTC.

No obstante, la FTC tan sólo se ha comprometido a tramitar prioritariamente los casos presentados por los organismos de autorregulación privados, como *BBBOnline* y *TRUSTe*, y de los Estados miembros de la Unión Europea que aleguen el incumplimiento de los principios de puerto seguro. Si la misma aprecia indicios de que se ha vulnerado el artículo 5 de la *Federal Trade Commission Act*, podría solucionar el asunto solicitando una decisión administrativa de cese de las prácticas denunciadas o presentando una denuncia ante un Tribunal Federal de Primera Instancia (*Federal District Couurt*).

Es necesario recalcar que los organismos de autorregulación privados propuestos por los Estados Unidos parecen cubrir únicamente las actividades online (*BBBOnline* y *TRUSTe*), motivo por el cual el GT29 ha mostrado su preocupación al respecto en opiniones como la Opinión 4/2000, de 16 de mayo del 2000[139]. En esta Opinión el

[137] Vid. Anexo VII de la Decisión de la Comisión de 26 de julio de 2000.

[138] "Se estima que más del 30 % de los miembros de puerto seguro no incluyen información sobre resolución de litigios en las políticas de privacidad que figuran en sus sitios web". Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE, de 27 de noviembre de 2013, COM (2013) 847 final, p. 9.

[139] "Alternative Dispute Resolution (although the existing bodies quoted by the US side seem to cover only "online" activities: BBB online, Webtrust and Trust-e)". Opinion 4/2000 on the level of protection provided by the "Safe Harbor Principles", adopte don 16th May 2000 (CA07/434/00/EN WP 32), p. 7.

GT29 subraya la incertidumbre que este sistema de resolución de conflictos provoca en el particular, pues si bien los organismos de autorregulación privados deberían notificar los casos de incumplimiento de los Principios a la FTC, no existe una obligación jurídica de hacerlo, y a pesar de que las personas afectadas pueden presentar sus quejas a la FTC, no hay garantía alguna de que la misma examine el caso, por gozar de poderes discrecionales[140].

Por lo tanto, cabe concluir que no existen 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.

2.2. La ineficacia del sistema de verificación que prevé la Pregunta más Frecuente número 7.

La FAQ número 7 detalla los dos tipos de procedimientos que pueden seguir las entidades adheridas al acuerdo de Puerto Seguro para verificar que los certificados y declaraciones que han presentado son ciertos, y que las prácticas se han aplicado de la manera indicada. En concreto, las para reunir los "requisitos de verificación" la entidad puede someterse, bien al procedimiento de "autoevaluación", o bien al procedimiento de "verificaciones por terceros".

Mediante el proceso de "autoevaluación" un directivo u otro representante autorizado de la empresa debe firmar un informe de verificación de la autoevaluación y presentarlo al Departamento de Comercio como mínimo una vez al año y éste debe difundirse a petición de los consumidores o en el contexto de posibles investigaciones o quejas por incumplimiento[141].

---

[140] De acuerdo con el GT29, "The "bridge" between the two layers is very uncertain: according to FAQ 11, the ADR bodies should notify to the FTC cases of failure to comply with the principles, but there is no obligation for them to do so. although the individuals concerned can complain directly to the FTC, there is no guarantee that the FTC will examine their case (its powers are discretionary). In concrete, individuals would not have the right to be heard before the FTC: neither to enforce the ADR bodies' decisions, nor to challenge such decisions (or the lack of decisions). As a result, the individuals concerned by an alleged violation of the principles would not be assured of the right to stand before an independent instance". Opinion 4/2000 on the level of protection provided by the "Safe Harbor Principles", adopte don 16th May 2000 (CA07/434/00/EN WP 32), p. 7.

[141] Vid. FAQ número 7 del Anexo II de la Decisión de la Comisión de 26 de julio de 2000.

Mayor efectividad suscita el proceso de "verificación por terceros", dado que pueden incluir auditorías, comprobaciones imprevistas, o el uso de herramientas tecnológicas. Sin embargo, cabe subrayar que la sumisión a este procedimiento es una mera facultad de que gozan las entidades adheridas al acuerdo de Puerto Seguro, pues sólo es aplicable "*cuando la entidad haya elegido someterse a la verificación por terceros*"[142]. Al igual que el de "autoevaluación", el informe que sea resultado de la "verificación por terceros" debe presentarse al Departamento de Comercio como mínimo una vez al año y difundirse a petición de los consumidores o en el contexto de posibles investigaciones o quejas por incumplimiento.

Lo dicho hasta aquí supone que la eficacia y la aplicación de los Principios de Puerto Seguro y de las FAQ se basa esencialmente en la auto-certificación de la FAQ número 6 y en la autoevaluación de la FAQ número 7, todo lo cual ha venido inquietando al GT29. En consecuencia, una entidad estadounidense adherida formalmente al Acuerdo de Puerto Seguro que infrinja manifiestamente los derechos fundamentales de los titulares de los datos procedentes de la UE no se verá obligada a modificar su conducta, y menos aún sancionada, hasta que no se investigue una denuncia[143].

Si después de tramitar la denuncia correspondiente, la FTC ve indicios de que se ha vulnerado el artículo 5 de la FTC, por existir una declaración falsa de adhesión a los principios de puerto seguro por parte la entidad autocertificada, puede solucionar el asunto emitiendo una decisión administrativa de cese de las prácticas denunciadas o presentar una denuncia ante un Tribunal Federal de Primera Instancia (*Federal District Court*). Si se quebrantan sus decisiones administrativas de cese, la FTC puede sancionar civilmente al incumplidor, y también puede ejercer acciones civiles o penales en los casos de incumplimiento de las resoluciones de los Tribunales Federales de Primera

[142] Vid. FAQ número 7 párrafo quinto.

[143] "As it stands, the "Safe Harbor" is a voluntary approach offered to US organisations on the basis of self-certification (FAQ 6) and self-assessment (FAQ 7), underpinned by statutory provisions in case of misrepresentation/deceptive practices. This means that, unless and until a complaint is made and investigated, any US organisation claiming the benefits of the "Safe Harbor" would be entitled to receive personal data from the EU". WP 27: Opinion 7/99 on the Level of Data Protection provided by the "Safe Harbor" Principles as published together with the Frequently Asked Questions (FAQs) and other related documents on 15 and 116 November 1999 by the US Department of Commerce, adopted on 3 December 1999 (5146/99/EN/final)", p. 2.

Instancia –todo ello poniéndolo en conocimiento del Departamento de Comercio de los EE.UU-[144].

Hay que mencionar, además, que tan sólo cuando la entidad adherida al acuerdo de Puerto Seguro efectúe un incumplimiento sistemático, cesa su derecho a beneficiarse del puerto seguro, siendo eliminada de la lista de entidades que posee el Departamento de Comercio, proporcionando éste a la entidad un plazo de 30 días para alegar lo que estime pertinente. De acuerdo con la Comunicación de la Comisión de 27 de noviembre de 2013, "la mayoría de las entidades retiradas de la lista de puerto seguro por el Departamento de Comercio lo fueron por petición propia (por ejemplo, entidades fusionadas o adquiridas por otras, que han cambiado su línea de negocio o que han cesado sus actividades)"[145].

A pesar de lo señalado con anterioridad, cabe remarcar que 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 UE y las empresas establecidas en la UE, de 27 de noviembre de 2013, la misma informó que "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 autocertificadas, lo que haría mucho más fiable el procedimiento de autocertificación"[146].

2.3. Los límites al ejercicio de los derechos de opción y de acceso en la Decisión de la Comisión de 26 de julio de 2000 y la formulación del principio de notificación.

Por una parte, de acuerdo con el derecho de opción o exclusión, las entidades deben ofrecer a los particulares la posibilidad de decidir si su información personal puede

[144] Vid. FAQ número 11 del Anexo II de la Decisión de la Comisión de 26 de julio de 2000.
[145] Vid. Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE, de 27 de noviembre de 2013, COM (2013) 847 final, p. 9.

[146] Vid. Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE, de 27 de noviembre de 2013, COM (2013) 847 final, p. 9.

divulgarse a un tercero o bien puede usarse para un fin incompatible con el objetivo inicial con el que fue recogida o no haya sido autorizado posteriormente por el particular. En opinión del GT29, los individuos deben tener la facultad de ejercer su derecho a opción o exclusión, no sólo cuando el nuevo objetivo se estima incompatible con el inicial, sino siempre que se utilice la información para un fin distinto[147].

Además, la FAQ número 1 establece un conjunto de excepciones al derecho de opción, y, en concreto, cuando se trata del tratamiento de datos especialmente protegidos. A la pregunta ¿debe una entidad ofrecer siempre de modo explícito la opción de participar cuando se trate de datos especialmente protegidos? La respuesta es negativa, al no ser necesario optar en los cinco supuestos enumerados por la FAQ.

Especial interés suscita la quinta excepción, según la cual el particular pierde su derecho de opción o exclusión cuando "*se refiere a información hecha pública de modo manifiesto por el particular",* y ello porque la información hecha pública continúa gozando del carácter de "dato personal". Ello que, si atendemos al Ordenamiento Jurídico Español, el artículo 3 j) de la LOPD, después de definir su término[148], enuncia con carácter de *numerus clausus* las cuatro fuentes de acceso público que se regirán por el estatus jurídico del artículo 11.2 de la LOPD, es decir cuando la comunicación de los datos personales contenidos en las mismas no hacen necesario el consentimiento por parte de su titular: en primer lugar, "*el censo promocional*"; en segundo lugar, "*los repertorios telefónicos en los términos previstos por su normativa específica*"; en tercer lugar, "*las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo*" y, por último, "*los diarios y boletines oficiales y los medios de comunicación*".

[147] "According to the "choice" principle, opt-out would be offered only where the "use or disclosure is incompatible with the purpose for which it [personal information] was originally collected or with any other purpose or disclosure identified in a notice to the individual". In its opinión 4 2/99, the Working Party has already stated and motivated its objections to such a narrow notion of "choice" and had made some suggestions for improvement". Opinion 4/99 on The Frequently Asked Questions to be issued by the US Department of Commerce in relation to the proposed "Safe Harbor Principles", adopte don 7 June 1999 (5066/99/EN/final WP 21), p. 3 y 4.

[148] Por fuentes accesibles al público se entiende "aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación".

Por otro lado, el derecho de acceso faculta a los particulares para acceder a información personal que las entidades tengan sobre ellos y poder corregir, modificar o suprimir dicha información si es inexacta.

Ahora bien, los sujetos titulares de los datos se hallan privados del ejercicio del derecho de acceso en dos supuestos[149]: por una parte, "*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*" y, por otra parte "*cuando puedan vulnerarse los derechos de otras personas*".

Dada la inconcreción del término "*carga o dispendio desproporcionado"*, en la FAQ número 8 se intenta delimitar el contenido de esta excepción, señalando que la obligación que tiene una entidad de proporcionar acceso a la información personal que posee sobre una persona se encuentra sujeta al principio de proporcionalidad o razonabilidad.

Después de citar varios ejemplos que pueden guiar a las entidades para denegar o admitir la solicitud de acceso a los datos personales de los afectados[150], y a pesar de remarcar que éstos "*no tienen que justificar las peticiones de acceso a sus propios datos*", de manera claramente contradictoria se añade que, al responder a las peticiones de acceso de los afectados, "*las entidades deben guiarse por los motivos de preocupación que provocaron inicialmente la petición*"[151], hecho que obliga a los afectados a justificar las peticiones de acceso a sus propios datos.

El derecho de acceso constituye un principio fundamental de cualquier régimen de protección pues, en palabras del GT29, "*access is the gateway which triggers all the rights of the data subject*; *it stresses that the exceptions to this fundamental principle are allowed only in exceptional circumstances; it reiterates the concern expressed in all its previous position papers with regard to the extent and the open-endedness of the*

[149] Vid. Principio de acceso del Anexo I de la Decisión de 26 de julio de 2000.
[150] Al tenor de la FAQ número 8, "si la información se está utilizando para tomar decisiones que afectarán significativamente a la persona (por ejemplo, la concesión o denegación de ventajas importantes, como un seguro, una hipoteca o un puesto de trabajo), de conformidad con los demás preceptos de estas FAQ, la entidad debería proporcionar la información aunque sea relativamente difícil o costoso".
[151] En la misma línea, la FAQ número 8 pone el siguiente ejemplo: "si una petición de acceso es vaga o muy amplia, la entidad puede dialogar con el afectado para comprender mejor los motivos de la petición y localizar la información correspondiente".

exceptions and conditions attached by the US side to the exercise of this fundamental right"[152].

A pesar de que la FAQ número 8 declara que "*las circunstancias por las que se puede denegar el acceso son limitadas*" y que "*las razones deben ser específicas*", ello es una mera declaración de intenciones, pues después de enumerar ocho causas que pueden comportar la denegación del acceso a los datos, se finaliza con una cláusula residual, que dice "*otras circunstancias en que la carga o dispendio necesarios para facilitar el acceso sean desproporcionados o se vulneren derechos o intereses legítimos de otras personas*".

También, en la FAQ número 8 se afirma que sí que existe un plazo para responder a las peticiones de acceso. No obstante, este plazo no está concretado, pues para su determinación meramente se dice que las entidades deben responder "*sin demoras excesivas y en un plazo de tiempo razonable*".

Sorprende además que la FAQ número 8 permite a las entidades cobrar una cuota a los particulares para cubrir el coste del derecho de acceso, "*siempre que no sea excesiva*", dificultando el ejercicio de un derecho fundamental a los particulares que no puedan costearlo. A los efectos de evitar esta situación de desprotección, en el ordenamiento jurídico español el artículo 15.1 de la LOPD prevé de forma expresa que "*el interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos*".

Por último, merece especial atención el modo en que se recoge el principio de notificación[153] en el Anexo I de la Decisión, que se halla en conexión con el derecho de

[152] Vid. Opinion 7/99 on the Level of Data Protection provided by the "Safe Harbor" Principles as published together with the Frequently Asked Questions (FAQs) and other related documents on 15 and 116 November 1999 by the US Department of Commerce, adopted on 3 December 1999 (5146/99/EN/final WP 27), p. 8.

[153] Como señala la Comisión en su Comunicación dirigida al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE, de 27 de noviembre de 2013, "un acceso insuficiente a las políticas de protección de la vida privada de dichas entidades perjudica a los particulares cuyos datos personales se estén recopilando y tratando, pudiendo constituir una infracción del principio de notificación. En tales casos es posible que los particulares cuyos datos se estén transfiriendo desde la UE no sean conscientes de sus derechos ni de las obligaciones a que está sujeta una entidad autocertificada". Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE, de 27 de noviembre de 2013,COM (2013) 847 final, p. 6.

acceso y de opción. En virtud de este principio, las entidades deben informar a los particulares de "*los fines con los que cuales recogen y utilizan información sobre ellos; la forma de contactar con ellas para cualquier pregunta o queja; los tipos de terceros a los cuales se revelará la información; las opciones y medios que la entidad ofrece a los particulares para limitar su uso y su divulgación*".

Posteriormente se procede a limitar el derecho a la notificación, apuntando que la notificación debe producirse "*la primera vez que se invite a los particulares a proporcionar a la entidad información personal o, posteriormente, tan pronto como sea posible, pero en cualquier caso antes de que la entidad use dicha información para un fin distinto de aquel con el que inicialmente la recogió o trató la entidad que la transfiere o la divulga por primera vez a un tercero*". Por lo que se refiere a la expresión "tan pronto como sea posible", el GT29 en su Opinión 2/99[154] ya apercibió a las autoridades norteamericanas de la necesidad de aclarar el significado exacto de este añadido, pues considera que el individuo debe ser informado en el momento de la recogida de los datos, y no a discreción de cada responsable del tratamiento.

2.4. La pérdida del control de los datos personales en las transferencias ulteriores.

Prosiguiendo con el análisis de la Decisión, conviene subrayar el régimen que la misma prevé con respecto a las transferencias o cesiones de datos personales que las entidades norteamericanas adheridas al acuerdo de Puerto Seguro realicen "a terceros", es decir, a otros responsables situados en los EE.UU que no se hayan adherido al acuerdo de Puerto Seguro, o bien localizados en otros lugares que pueden no ofrecer una protección adecuada de los datos.

Al tenor del Principio denominado "transferencia ulterior", contenido en el Anexo I de la Decisión, para revelar datos personales a "terceros" las entidades norteamericanas deben cumplir con dos presupuestos: por una parte, deben aplicar los principios de notificación y opción y, por otra parte, deben asegurarse de que el importador de los

---

[154] "The Working Party also seeks clarification as to the exact meaning of the expression "or as soon thereafter practicable", as it considers that the individual should be informed at the time of collection and not at the discretion of each controller". WP 19: Opinion 2/99 on the Adequacy of the "International Safe Harbor Principles" isued by the US Department of Commerce on 19th April 1999, adopte don 2 May 1999 (5047/99/EN/final), p.5.

datos suscribe los principios, o bien firmar con él un convenio por escrito para que ofrezca como mínimo el mismo nivel de protección de la vida privada que el requerido por dichos principios.

Si bien "formalmente" parece correcta esta previsión, es necesario recalcar que ninguna autoridad pública asume la competencia de controlar que tales presupuestos se cumplan en la práctica. Basta recordar que el artículo 33.1 de la LOPD señala que, para realizar transferencias internacionales de datos a Estados que no ofrezcan un nivel de protección adecuado de los mismos, sebe obtenerse "*autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas*", siendo éste el precepto que transpone el artículo 26.2 de la Directiva 95/46/CE[155].

Hay que mencionar, además, que una vez la entidad norteamericana adherida al acuerdo de Puerto Seguro ha celebrado este "convenio", que debería ofrecer las garantías contenidas en los Principios, pero que puede no ofrecerlo –pues ninguna autoridad pública norteamericana evalúa el contenido de este "convenio"-, la entidad exportadora "*no será responsable (a menos que la propia entidad acuerde lo contrario) del tratamiento realizado por el tercero a quien haya transferido este tipo de información y que vulnere las limitaciones o estipulaciones establecidas, a menos que la entidad sepa, o debiera saber, que el tercero realizaría dicho tratamiento y no haya adoptado medidas razonables para impedir o detener tal tratamiento*"[156].

Lo dicho hasta aquí supone que el particular cuyos datos personales vayan a ser objeto de una transferencia por parte de entidades adheridas al Puerto Seguro pierde el control de sus propios datos de forma definitiva, de ahí que resulte esencial, en estos supuestos, el cumplimiento de los principios de notificación y opción –los cuales, a su vez, se hallan sumamente limitados y sujetos a numerosas excepciones, tanto en los

[155]De acuerdo con el artículo 26 apartado 2 de la Directiva 95/46/CE, "*los Estados miembros podrán autorizar una transferencia o una serie de transferencias de datos personales a un tercer país que no garantice un nivel de protección adecuado con arreglo al apartado 2 del artículo 25, cuando el responsable del tratamiento ofrezca garantías suficientes respecto de la protección de la vida privada, de los derechos y libertades fundamentales de las personas, así como respecto al ejercicio de los respectivos derechos; dichas garantías podrán derivarse, en particular, de cláusulas contractuales apropiadas*".

[156] Vid. Principio de transferencia ulterior del Anexo I de la Decisión de la Comisión de 26 de julio de 2000.

Principios como en las FAQ. La necesidad de cumplir con el derecho de opción es remarcada por el GT29 en opiniones como la Opinión 2/99[157].

2.5. El papel de las autoridades nacionales de supervisión de los Estados miembros de la UE.

Como podemos observar en la FAQ número 5, las agencias europeas de protección de datos pueden ejercer competencias de "información y asesoramiento" a las entidades estadounidenses involucradas en quejas no resueltas de particulares relacionadas con la información personal transferida desde la UE en el ámbito del Puerto Seguro, a través de un "panel informal de APD de ámbito europeo"[158].

Cabe añadir, además, que las entidades adheridas al acuerdo de Puerto Seguro gozan de la "facultad" de comprometerse a colaborar con las autoridades de protección de datos de la UE, para lo cual deben declararlo en su certificación de Puerto Seguro dirigida al Departamento de Comercio. Ello implica, por una parte, que las mismas deben colaborar con las autoridades de protección de datos europeas en la investigación y resolución de quejas que se formulen con arreglo al Puerto Seguro y, por otra parte, implica el nacimiento de una obligación para las entidades de cumplir con las decisiones de dichas autoridades europeas, cuando éstas determinen que la entidad debe tomar medidas concretas para cumplir con los Principios y las FAQ –como por ejemplo el pago de indemnizaciones o compensaciones-.

Si ya limita la efectividad de esta previsión el que sean las entidades quienes voluntariamente decidan colaborar con autoridades europeas, conviene subrayar que el GT29 observa que las autoridades nacionales de supervisión de la UE, al tenor de la

[157] "Although not present in OECD guidelines, this principle is necessary to ensure that data is not transferred by a US company that abides by the Safe Harbor Principles to another controller in the US or indeed elsewhere not offering adequate protection. But as presently drafted, it is not clear what the applicable rule is. We understand that the individual should be able to opt out of a transfer to a third party. To this end, he needs at least the information that data shall be transferred and whether or not the third party adheres to the safe harbor principles or how adequate protection is provided otherwise. The Working Party therefore supports the Commission's request expressed in footnote 5 that explicit notice and choice are to be provided when personal data is transferred to a third party that does not adhere to the Safe Harbor Principles". Opinion 2/99 on the Adequacy of the "International Safe Harbor Principles" isued by the US Department of Commerce on 19th April 1999, adopte don 2 May 1999 (5047/99/EN/final WP 19), p. 5 y 6.

[158] La FAQ número 5 señala que esta actividad de asesoramiento tendrá como finalidad la correcta aplicación de los principios de puerto seguro y conllevará la indemnización de los afectados que las APD consideren adecuada.

normativa que las regula, no gozan de competencia en terceros Estados, motivo por el cual carecen de las competencias ejecutivas que les permitirán supervisar eficazmente la aplicación de los Principios y las FAQ por las entidades estadounidenses[159].

Además, al tenor del artículo 3.1 de la Decisión, las autoridades competentes de los Estados miembros pueden ejercer su facultad de suspender los flujos de datos hacia una entidad autocertificada cuando la FTC, el Departamento de Transporte o los mecanismos alternativos de resolución de conflictos hayan resuelto a misma ha vulnerado los principios y su aplicación de conformidad con las FAQ, o cuando existen grandes probabilidades de que se estén vulnerando los principios, entre otros supuestos[160].

III. PROBLEMAS EN LA APLICACIÓN DE LOS PRINCIPIOS DE PUERTO SEGURO Y DE LAS PREGUNTAS MÁS FRECUENTES.

1. Un nuevo contexto de desarrollo de la economía digital.

El primer problema que cabe esgrimir con respecto a la aplicación de la Decisión de la Comisión de 26 de julio del 2000 es el profundo cambio que la "economía digital" ha comportado en el derecho fundamental a la protección de los datos personales. Desde el año 2000 se ha venido produciendo un aumento exponencial de la cantidad, calidad, diversidad y naturaleza de las actividades de tratamiento de datos, especialmente en la economía transatlántica y ha crecido notablemente el número de empresas de Estados Unidos adheridas al acuerdo de Puerto Seguro –pasando de 400 entidades en 2004 a

[159] En este sentido, de acuerdo con el Grupo de Trabajo del artículo 29, "with regard to the possibility for organisations adhering to the Department of Commerce's principles to rely on National Supervisory authorities for the implementation of the Principles, the Working Party notes that National supervisory authorities do not have jurisdiction in third countries and consequently lack any enforcement powers which would allow them to oversee effectively the implementation of the Principles by US organisations. Opinion 2/99 on the Adequacy of the "International Safe Harbor Principles" isued by the US Department of Commerce on 19th April 1999, adopte don 2 May 1999 (5047/99/EN/final WP 19), p. 3.

[160] También si "existen razones para creer que el mecanismo de aplicación correspondiente no ha tomado o no tomará las medidas oportunas para resolver el caso en cuestión; la continuación de la transferencia podría crear un riesgo inminente de grave perjuicio a los afectados; y las autoridades competentes del Estado miembro han hecho esfuerzos razonables en estas circunstancias para notificárselo a la entidad y proporcionarle la oportunidad de alegar.

3.246 en 2013, más de la mitad de las cuales se han adherido al mismo en los últimos cinco años-[161].

Así mismo, forman parte de los intercambios comerciales entre la UE y EE.UU. nuevos sectores digitales que se hallan en crecimiento, tales como las redes sociales o la computación en la nube (ampliamente conocido como "*cloud computing*"[162]), que implican la transferencia de grandes cantidades de datos de la UE a EE.UU.

Como bien señala la Comisión Europea en su Comunicación al Parlamento Europeo y al Consejo, sobre restablecer la confianza en los flujos de datos entre la UE y EE.UU, de 27 de noviembre de 2013, "ha aumentado el uso de los servicios de comunicación electrónica por parte de los ciudadanos en su vida cotidiana", convirtiéndose los datos personales "en un activo de gran valor". En la Comunicación se detalla, por una parte, que el valor estimado de los datos de los ciudadanos de la UE fue de 315 000 millones de euros en 2011 y tiene un potencial de crecimiento de casi 1 billón de euros al año hasta 2020 y, por otra parte, conviene remarcar que "el mercado de análisis de grandes conjuntos de datos está aumentando en un 40 % anual a nivel mundial" [163].

2. La falta de transparencia y de control en la ejecución del régimen de puerto seguro y su incumplimiento por las empresas autocertificadas.

Al tenor de 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 UE y las empresas establecidas en la UE, de 27 de noviembre de 2013, esta Institución europea constató que, a lo largo de los años, un número importante de entidades

[161] Vid. Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE, de 27 de noviembre de 2013, p.3.

[162] A título ilustrativo puede citarse la estadística realizada por el *Center on Law and Information Policy* de *Fordham Law School*, en el ámbito educativo"el 95% de los distritos dependen de los servicios en la nube para una amplia gama de funciones, incluyendo datos relacionados con el rendimiento de los estudiantes, el apoyo a las actividades de clase, orientación al estudiante, así como la utilización de servicios especiales, tales como los pagos de la cafetería y la planificación del transporte". REIDENBERG, Joel R.; RUSSELL, N. Cameron, entre otros, *Privacy and Cloud Computing in Public Schools*, Center on Law and Information Policy, 2013, p. 5.

[163] Vid. Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre restablecer la confianza en los flujos de datos entre la UE y EE.UU, de 27 de noviembre de 2013. COM (2013) 846 final, p. 3.

autocertificadas no habían hecho pública su política de protección de la vida privada o no habían declarado públicamente su adhesión a los principios de puerto seguro[164].

A ello debe añadirse que las políticas de privacidad de las entidades no siempre se han presentado de forma que facilite la lectura y sean comprensibles para el consumidor medio, e incluso, en determinados supuestos, los hipervínculos a las políticas de protección de la vida privada no funcionaban correctamente ni remitían a las páginas web correspondientes.

De acuerdo con la Comisión, estadísticas correspondientes al año 2013 ponían de manifiesto la existencia de alegaciones falsas de adhesión al puerto seguro. En este sentido, en torno a un 10 % de las entidades que afirmaban ser miembros de este marco realmente no figuraban en la actual lista de miembros del Departamento de Comercio de EEUU. Así, tales afirmaciones falsas procedían tanto de entidades que nunca habían participado en el marco de Puerto Seguro como de entidades que se habían adherido a él, pero posteriormente no enviaron la renovación anual de su autocertificación al Departamento de Comercio[165].

En lo que al ámbito de la tutela judicial efectiva se refiere, la Comisión constató que en los últimos tres años –es decir, del 2010 al 2013-, las autoridades europeas de protección de datos habían enviado muy pocos casos a la Comisión Federal del Comercio[166]. Además, la Comisión cuestionó la efectividad de los tres principales mecanismos de recurso previstos en el régimen de Puerto Seguro –el panel de protección de datos de la UE, el BBB (*Better Business Bureaus*) y *TRUSTe*- pues hasta el 2013 tan sólo habían tratado un número muy limitado de casos. Por ejemplo, describe la Comisión que "uno de los mayores proveedores de servicios (*TRUSTe*) comunicó que en 2010 había recibido 881 peticiones, pero que sólo tres se consideraron admisibles y fundadas y tuvieron como consecuencia que se obligase a la entidad en cuestión a modificar su política de protección de la vida privada (…) y según el Departamento de Comercio, la gran mayoría de las quejas que piden una solución extrajudicial proceden

[164] Vid. Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE, de 27 de noviembre de 2013, COM (2013) 847 final, p. 7.
[165] Vid. Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE, de 27 de noviembre de 2013, COM (2013) 847 final, p. 8.
[166] Vid. Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE, de 27 de noviembre de 2013, COM (2013) 847 final, p. 12.

de consumidores, por ejemplo, usuarios que olvidan su contraseña y no pueden obtenerla a través del servicio de internet" [167].

3. La vigilancia de las comunicaciones electrónicas a los efectos de inteligencia y seguridad nacional en Estados Unidos de América.

El 5 de junio de 2013 el periódico británico *The Guardian* informó sobre las actividades de vigilancia llevadas a cabo por los servicios de inteligencia de Estados Unidos, basándose en la documentación suministrada por Edward Snowden, antiguo trabajador de la *National Security Agency* ("NSA"). De acuerdo con este artículo, las comunicaciones de millones de ciudadanos estaban siendo recogidas de forma indiscriminada, sin importar si eran sospechosos de cometer crimen alguno.

Con posterioridad, el Gobierno de EE.UU[168] reconoció la existencia de un "programa", en virtud del cual el *Federal Bureau of Investigation* (en adelante, "FBI") venía obteniendo órdenes de la *Foreign Intelligence Surveillance Court* (en adelante, "FISC"), de conformidad con la Sección 215 de la USA PATRIOT Act, de dirigir copias electrónicas de los registros de llamadas recogidos por ciertos proveedores de servicios de telecomunicaciones.

Los medios de comunicación[169] también revelaron la existencia de otros programas de vigilancia del Gobierno de EE.UU, como el programa "*PRISM*" [170], cuyo objeto ha

[167] Vid. Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE, de 27 de noviembre de 2013, COM (2013) 847 final, p. 15.

[168] Vid. EL PAÍS, Imperialismo digital, EEUU usa la información para proteger su economía y el éxito depende de la pasividad de sus víctimas, 1 de noviembre de 2013, en línea: http://internacional.elpais.com/internacional/2013/11/01/actualidad/1383333227_605243.html [consultado el 1.05.2016].

[169] "El Gobierno de Barack Obama no sólo tiene información sensible de millones de llamadas telefónicas, también tiene acceso directo a los datos y a los servidores de todopoderosas empresas de Internet como Google, Facebook o Apple. Una presentación en Powepoint de la Agencia de Seguridad Nacional (NSA) a la que ha tenido acceso los diarios 'The Guardian' y 'The Washington Post' probaría el control de EEUU sobre el contenido de determinados e-mails, fotografías, vídeos conversaciones de chat o transferencia de archivos". EL MUNDO, EEUU "espía" a través de los servidores de Apple, Google o Facebook, en línea: http://www.elmundo.es/america/2013/06/07/estados_unidos/1370577062.html [consultado el 20.04.2016].

[170] Las reacciones a la utilización del programa de espionaje masivo por parte de la NSA también llegan de otras partes del mundo, (…) la propia presidenta de Brasil, Dilma Rousseff, (…) aprovechaba su intervención ante la Asamblea General de Naciones Unidas para denunciar estas prácticas de espionaje internacional, que definición como un atentado a la «soberanía de los Estados» y a la «libertad de expresión» y como una «violación de los derechos humanos», y proponer una regulación que asegure un mayor control del uso de Internet para evitar este tipo de actividades de vigilancia. Según ha publicado

sido recopilar datos personales relacionados con Internet[171]. En este sentido, sorprende la constatación efectuada por la Comisión en su Comunicación de 27 de noviembre de 2013, según la cual "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"[172].

Es de gran interés la información contenida en el *Memorandum opinion* de *United States District Court for the District of Columbia*, emitido el 16 de diciembre de 2013[173]. En este documento se expone que, tras estas revelaciones, en EE.UU se sustanciaron dos procedimientos –el 2 de junio de 2013 el caso *Klayman I* y el 12 de junio de 2013 el caso *Klayman II*-, cuyas partes demandantes alegaron que el Gobierno, con la participación de compañías privadas, estaba efectuando "*a secret and ilegal government scheme to intercept and analyze vast quantities of domestic telephonic communications and of communications from the Internet and electronic service providers*" [174]. Por lo que se refiere a la parte demandada, las acciones se ejercitaron contra el Gobierno norteamericano, así como contra Facebook, Yahoo, Google, Microsoft, Youtube, AOL, PalTalk, Skype, Sprint, AT&T, and Apple, afirmando que los afectados son los subscriptores, usuarios, consumidores de estos proveedores de servicios, los cuales han visto violados sus derechos individuales recogidos bajo la Primera, la Cuarta y la Quinta Enmienda de la Constitución, vulnerándose además la *Administrative Procedure Act* ("APA")[175], pues el Gobierno se ha excedido de su potestad legal bajo la *Foreign Intelligence Surveillance Act* (en adelante, "FISA").

The New York Times, en los últimos años la NSA ha desarrollado un complejo sistema que permite cruzar información personal procedente de llamadas telefónicas, correos electrónicos, geolocalización, perfiles de redes sociales o datos bancarios, para elaborar perfiles capaces de predecir la conducta de los titulares de esos datos. REDACCIÓN DIARIO LA LEY, "Las explicaciones de EE.UU. sobre el programa de espionaje masivo no convencen a la UE", *Diario La Ley*, nº 8175, (2013), p. 2.

[171] Vid. THE GUARDIAN, *NSA Prism program taps in to user data of Apple, Google and others*, 6 de junio de 2013, en línea: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data [consultado el 03.04.2016].

[172] Vid. Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE, de 27 de noviembre de 2013, COM (2013) 847 final, p. 17.

[173] Vid. *Memorandum opinion* of *United States District Court for the District of Columbia*, de 16 de diciembre de 2013 (Civil Action No. 13-0851).

[174] Vid. *Memorandum opinion* of *United States District Court for the District of Columbia*, de 16 de diciembre de 2013 (Civil Action No. 13-0851), p. 8.

[175] The APA "establishes a cause of action for those suffering legal wrong because of agency action, or adversely affected or aggrieved by agency action (…). In particular, the APA permits such aggrieved persons to bring suit agains the United States and its officers for relief other tan money damages". *Memorandum opinion* of *United States District Court for the District of Columbia*, de 16 de diciembre de 2013 (Civil Action No. 13-0851), p. 24.

En 1978 el Congreso de EE.UU promulgó la *Foreign Intelligence Surveillance Act*[176], ampliamente conocida como "FISA", para autorizar y regular ciertas actividades de vigilancia gubernamental de las comunicaciones, a los efectos de inteligencia extranjera. En concreto, se estipuló el procedimiento que debía seguir el Gobierno para obtener órdenes judiciales autorizando las vigilancias electrónicas en el ámbito doméstico, así como se creó la *Foreign Intelligence Surveillance Court* o FISC y la *FISC Court of Review*, ambas con jurisdicción para responder a las peticiones efectuadas en el ámbito de la FISA.

Por otra parte, la Sección 1861 también impone otros requisitos al FBI para el caso que pretenda ejercer esta potestad de vigilancia[177]. Conforme a la Sección 1961, el Gobierno desarrolló un "programa de lucha contra el terrorismo" ("*a counterterrorism program*"), denominado "*Bulk Telephony Metadata Program*", mediante el cual recogía, almacenaba, conservaba y analizaba "metadatos" contenidos en registros de llamadas telefónicas de muchas compañías de telecomunicaciones. Deseo subrayar que los "metadatos" utilizados por este programa eran los números de teléfono utilizados para hacer y recibir llamadas, la hora y el día en que las mismas tenían lugar, así como la duración de dichas llamadas.

Al tenor de las alegaciones efectuadas por el Gobierno de EE.UU, estos registros de "metadatos" no incluyen información alguna sobre el contenido de estas llamadas. Así mismo, la agregación de los mismos a bases de datos permite a la NSA analizar las conexiones entre los números que razonablemente podían ser sospechosos de hallarse asociados con actividades terroristas u otros números desconocidos[178].

[176] FISA was "in large measure a response to the revelations that warrantless electronic surveillance in the name of national security has been seriously abused (…) In the view of the Senate Judiciary Comitteem the act went a long way in striking a fair and just balance between protection of national security and protection of personal liberties". *Memorandum opinion* of *United States District Court for the District of Columbia*, de 16 de diciembre de 2013 (Civil Action No. 13-0851), p. 9.

[177] Under Section 1861's "use" provision, information that FBI acquires through succh a production order "concerning any US person may be used and disclosed by Federal officers and employees without the consent of the US person only in accordance with the minimization procedures adopted by the Attorney General and approved by the FISC. *Memorandum opinion* of *United States District Court for the District of Columbia*, de 16 de diciembre de 2013 (Civil Action No. 13-0851), p. 13.

[178] This agreggation of records into a single database creates "an historical repository that permits retrospective analysis (…) enabling NSA analysts to draw connections, across telecommunications service providers, between numbers reasonably suspected to be associated with terrorist activity and with other, unknown numbers". *Memorandum opinion* of *United States District Court for the District of Columbia*, de 16 de diciembre de 2013 (Civil Action No. 13-0851), p. 17.

Con miras a concretar el concepto de "metadatos" resulta de interés lo que se señala en el Dictamen 04/2014 del Grupo de Trabajo del Artículo 29, sobre la vigilancia de las comunicaciones a efectos de inteligencia y seguridad nacional, adoptado el 10 de abril de 2014. Si bien suele alegarse que la recogida de metadatos es "menos grave" que recoger los contenidos de la información, dicho dictamen concluye que ello no es así. En primer término, si bien los metadatos son "todos los datos sobre una comunicación en curso, excepto el contenido de la conversación"[179], su análisis puede revelar datos delicados sobre las personas, como pueden ser las llamadas a determinados números de información médica o centros religiosos.

En segundo lugar, el análisis de los metadatos suele aportar información de forma más sencilla que el análisis de los propios contenidos de las comunicaciones, pues "unos complejos instrumentos informáticos permiten analizar grandes conjuntos de datos para identificar modelos y relaciones incorporados, incluidos a datos personales, hábitos y comportamientos"[180] –lo cual no sucede en las conversaciones, que pueden desarrollarse en cualquier forma o idioma-.

Por último, deseo remarcar que el artículo 2 a) de la Directiva 95/46/CE define el concepto de "datos personales" como "*toda información sobre una persona física identificada o identificable*", motivo por el cual en la Unión Europea los "metadatos" son datos personales y, por lo tanto, deben hallarse protegidos.

Prosiguiendo con el análisis de la actividad de vigilancia efectuada por el Gobierno de EEUU, en 2009 el Juez Reggie Walton de la FISC concluyó que la NSA, tras la creación del *Bulk Telephony Metadata Program,* había protagonizado un incumplimiento sistemático de los procedimientos exigidos por la normativa[181]. Conviene remarcar que, a diferencia de las bases de datos que recopilan huellas dactilares, que tan sólo recopilan una única imprenta de la huella dactilar de cada

[179] Pueden "incluir el número de teléfono o dirección IP de la persona que hace la llamada o envía un correo electrónico, el tiempo y la información relativa a la ubicación, el asunto, el destinatario, etcétera". Dictamen 04/2014 del Grupo de Trabajo del Artículo 29, sobre la vigilancia de las comunicaciones a efectos de inteligencia y seguridad nacional, adoptado el 10 de abril de 2014 (819/14/EN WP 215), p. 4.

[180] Vid. Dictamen 04/2014 del Grupo de Trabajo del Artículo 29, sobre la vigilancia de las comunicaciones a efectos de inteligencia y seguridad nacional, adoptado el 10 de abril de 2014 (819/14/EN WP 215), p. 5.

[181] Vid. *Memorandum opinion* of *United States District Court for the District of Columbia*, de 16 de diciembre de 2013 (Civil Action No. 13-0851), p. 21.

persona, las bases de datos de la NSA se actualizan día tras día, con nueva información sobre cada número de teléfono[182].

Si bien podría alegarse que esta vigilancia de las comunicaciones telefónicas podría ser contraria a la Cuarta Enmienda de la Constitución de EEUU, el *Memorandum opinion* de *United States District Court for the District of Columbia*, de 16 de diciembre de 2013 recuerda que, en virtud del caso *Smith v. Maryland* la Corte Suprema de EEUU sostuvo que no había una expectativa razonable de privacidad con respecto a la información que se transmite a la compañía telefónica. Por lo tanto, de acuerdo con este precedente el *Bulk Telephony Metadata Program* no gozaría de la protección de la Cuarta Enmienda.

En el *Memorandum opinion* se remarca que ello no debería ser así, pues han evolucionado las capacidades de vigilancia del Gobierno norteamericano, así como los hábitos de los ciudadanos y la relación entre la NSA y las compañías de telecomunicaciones: "*Nor could the Court in 1979 have ever imagined how the citizens of 2013 would interact with their phones (…), 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 assessin whether the Bulk Telephony Metadata Program constitutes a Fourth Amendment search*" [183].

Por último, deseo subrayar que los programas de vigilancia secretos, masivos e indiscriminados utilizados por el Gobierno de Estados Unidos son incompatibles con las leyes fundamentales de la Unión Europea y no pueden justificarse por motivos de lucha contra el terrorismo u otras importantes amenazas a la seguridad nacional[184].

Para que las excepciones a la aplicación del régimen de Puerto Seguro por aplicación de la ley de EEUU o defensa de seguridad nacional fueran válidas, apunta la Comisión en su Comunicación al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro, de 27 de noviembre de 2013 que, "para ser válidas,

[182] "Because the Government can use daily metadata collection to engage in repetitive, surreptitious surveillance of a citizen's private goings on, the NSA database implicates the Fourth Amendment each time a government oficial monitors it". *Memorandum opinion* of *United States District Court for the District of Columbia*, de 16 de diciembre de 2013 (Civil Action No. 13-0851), p. 41.

[183] Vid. *Memorandum opinion* of *United States District Court for the District of Columbia*, de 16 de diciembre de 2013 (Civil Action No. 13-0851), p. 45.

[184] Vid. Dictamen 04/2014 del Grupo de Trabajo del Artículo 29, sobre la vigilancia de las comunicaciones a efectos de inteligencia y seguridad nacional, adoptado el 10 de abril de 2014 (819/14/EN WP 215), p. 2.

las limitaciones y restricciones al disfrute de los derechos fundamentales deben interpretarse restrictivamente, deben presentarse en una legislación accesible al público y deben ser necesarias y proporcionadas en una sociedad democrática"[185].

IV. LA SENTENCIA DEL TRIBUNAL DE JUSTICIA DE LA UNIÓN EUROPEA, DE 6 DE OCTUBRE DE 2015.

En virtud de la Sentencia del Tribunal de Justicia de la Unión Europea, de 6 de octubre de 2015[186] se invalidó la Decisión de la Comisión 2000/520, de 26 de julio, sobre la adecuación conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes. A continuación se procederá a analizar las razones que llevaron al TJUE a declarar la invalidez de la Decisión.

1. Antecedentes de hecho de la Sentencia del Tribunal de Justicia de la Unión Europea, de 6 de octubre de 2015.

En el supuesto de hecho de la Sentencia, el Maximillian Schrems, nacional austriaco residente en Austria que era usuario de la red Facebook de 2008, presentó una reclamación ante el *Data Protection Commissioner* el 25 de junio de 2013 solicitando que prohibiera a *Facebook Ireland* transferir sus datos personales a EE.UU[187], pues estimaba que las prácticas en vigor en dicho país no garantizaban una protección suficiente de los datos personales conservados en su territorio. Hay que mencionar, además, que el Sr. Schrems hizo referencia a las revelaciones del Sr. Edward Snowden sobre las actividades de los servicios de información de Estados Unidos, en particular las de las *National Security Agency* (en adelante, "NSA").

[185] Vid. Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE, de 27 de noviembre de 2013, COM (2013) 847 final, p. 18

[186] Vid. Sentencia del Tribunal de Justicia de la Unión Europea, de 6 de octubre de 2015, en el asunto C-362/14, que tiene por objeto una petición 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 Data Protection Commissioner.

[187] Cabe destacar que toda persona residente en el territorio de la Unión que desee utilizar Facebook está obligada a concluir en el momento de su inscripción un contrato con Facebook Ireland, filial de Facebook Inc., domiciliada ésta última en Estados Unidos. Los datos personales de los usuarios de Facebook Ireland residentes en el territorio de la Unión se transfieren en todo o en parte a servidores pertenecientes a Facebook Inc, situados en el territorio de Estados Unidos, donde son objeto de tratamiento. Sentencia del Tribunal de Justicia de la Unión Europea, de 6 de octubre de 2015, en el asunto C-362/14, fragmento número 27.

El Comisario desestimó la reclamación por estimarla "infundada", pues apreció que "no había pruebas de que la NSA hubiera accedido a los datos personales del interesado" y que "el carácter adecuado de la protección de los datos personales en EE.UU. debía resolverse conforme a la Decisión de la Comisión de 26 de julio de 2000". Posteriormente, el Sr. Schrems interpuso un recurso ante la *High Court* de Irlanda.

Al estimar la *High Court*[188] que la legalidad de la Decisión de la Comisión de 26 de julio de 2000 debía apreciarse a la luz del Derecho de la Unión, decidió suspender el procedimiento y plantear al Tribunal de Justicia de la Unión Europea (en adelante, "TJUE") dos cuestiones prejudiciales. En primer lugar, si el Comisario, a pesar de apreciar que la legislación y práctica de un tercer país no prevén una protección adecuada de los datos personales, se halla vinculado en términos absolutos por la Decisión y, en segundo lugar, si el comisario puede o debe realizar su propia investigación a la luz de los hechos que han tenido lugar desde la publicación de dicha Decisión.

2. Sobre la validez de la Decisión 2000/520.

El TJUE inicia su fundamentación jurídica recordando que las Decisiones que la Comisión Europea puede adoptar con fundamento en el artículo 25.6 de la Directiva 95/46/CE tienen como destinatarios los Estados miembros, los cuales deberán adoptar las medidas necesarias para atenerse a ella, pues su aplicación tiene carácter obligatorio y vinculante al tenor del artículo 288 del Tratado de Funcionamiento de la Unión Europea[189].

[188] La *High Court* señaló que "una vez transferidos los datos personales a Estados Unidos, la NSA y otros organismos federales, como el *Federal Bureau of Investigation* (FBI), pueden acceder a ellos en el contexto de la vigilancia y de las interceptaciones indiferenciadas que ejecutan a gran escala"[188] y que "el acceso masivo e indiferenciado a los datos personales es manifiestamente contrario al principio de proporcionalidad y a los valores fundamentales protegidos por la Constitución irlandesa", pues para que las interceptaciones de comunicaciones electrónicas puedan ser acordes a derecho, "debe aportarse la prueba de que esas interceptaciones tienen carácter selectivo, de que la vigilancia de determinadas personas o de determinados grupos de personas está objetivamente justificada en interés de la seguridad nacional o de la represión de la delincuencia".

[189] De acuerdo con el artículo 288 apartado 4 del TFUE, "la decisión será obligatoria en todos sus elementos. Cuando designe destinatarios, sólo será obligatoria para éstos".

Como se apunta en el fragmento 52 de la Sentencia que ahora se analiza, dado que los actos de las instituciones de la Unión disfrutan en principio de una presunción de legalidad, "mientras la decisión de la Comisión no haya sido declarada inválida por el Tribunal de Justicia, los Estados miembros y sus órganos, entre ellos las autoridades de control independientes, no pueden ciertamente adoptar medidas contrarias a esa decisión, como serían actos por los que se apreciara con efecto obligatorio que el tercer país al que se refiere dicha decisión no garantiza un nivel de protección adecuado".

A los efectos de examinar la validez de la Decisión, el TJUE hace referencia a que, si bien "no cabe exigir que un tercer país garantice un nivel de protección idéntico al garantizado en el ordenamiento jurídico de la Unión"[190], sí que es exigible que ese tercer país "garantice efectivamente, por su legislación interna o sus compromisos internacionales" –como criterios que establece el artículo 25.6 de la Directiva 95/46/CE-, "un nivel de protección de las libertades y derechos fundamentales sustancialmente equivalente al garantizado en la Unión por la Directiva 95/46"[191], siendo el "ordenamiento jurídico del tercer país" el que debe garantizar el nivel adecuado de protección.

Del análisis de la Sentencia del Tribunal de Justicia de la Unión Europea, de 6 de octubre de 2015, cabe extraer que el Tribunal esgrime seis razones fundamentales para declarar la invalidez de la Decisión.

Empezando por el análisis de la validez del artículo 1 de la Decisión, el TJUE aclara que, si bien el sistema de autocertificación que se utiliza en la Decisión de 26 de julio de 2000 no es por sí mismo contrario a la exigencia enunciada en el artículo 25.6 de la Directiva 95/46/CE, la fiabilidad de este mecanismo descansa "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"[192].

Estos requisitos de "fiabilidad" del sistema no se han venido dando en la práctica pues, en primer lugar, dado que los principios son aplicables únicamente a las entidades

[190] Vid. Sentencia del Tribunal de Justicia de la Unión Europea, de 6 de octubre de 2015, en el asunto C-362/14, fragmento número 73.
[191] Vid. Sentencia del Tribunal de Justicia de la Unión Europea, de 6 de octubre de 2015, en el asunto C-362/14, fragmento número 73.
[192] Vid. Sentencia del Tribunal de Justicia de la Unión Europea, de 6 de octubre de 2015, en el asunto C-362/14, fragmento número 81.

estadounidenses que se han adherido voluntariamente al acuerdo de Puerto Seguro y reciben datos personales desde la Unión, las autoridades públicas estadounidenses no se hallan obligadas al cumplimiento de estos principios, motivo por el cual las mismas pueden incumplirlo en aplicación de la ley estadounidense. En segundo lugar, la Decisión no contiene las constataciones suficientes sobre las medidas con las que Estados Unidos garantiza un nivel de protección adecuado, lo cual es exigible en virtud del artículo 25.6 de la Directiva 95/46/CE.

En tercer lugar, es también causa de invalidez de la Decisión el que la aplicabilidad de los Principios y las FAQ –al tenor del Anexo I párrafo cuarto de la Decisión- pueda limitarse por las exigencias de seguridad nacional, interés público y cumplimiento de la ley de Estados Unidos, así como por disposición legal o reglamentaria, o jurisprudencia, que originen conflictos de obligaciones o autorizaciones explícitas. Ello evidencia una clara primacía con respecto a los intereses nacionales de EE.UU queda patente también en el título B del Anexo IV de la Decisión, al remarcar éste que "es evidente que, si la legislación estadounidense establece una obligación en contrario, las entidades deben cumplirla, dentro o fuera del ámbito de los principios de puerto seguro".

En cuarto lugar, al establecimiento de dicha primacía debe agregarse que la Decisión no contiene ninguna constatación sobre la existencia en Estados Unidos de reglas estatales destinadas a limitar las posibles injerencias en los derechos fundamentales de las personas cuyos datos se transfieran desde la Unión a Estados Unidos[193].

En lo que a los mecanismos de arbitraje privado y los procedimientos ante la Comisión Federal de Comercio, el TJUE apunta, en quinto lugar, que los mismos se limitan a los litigios comerciales y no se pueden aplicar en litigios concernientes a la legalidad de injerencias en los derechos fundamentales derivadas de medidas de origen estatal[194].

Esta regulación poco protectora implicó que las autoridades estadounidenses pudiesen acceder a los datos personales transferidos a partir de los Estados miembros a Estados Unidos y tratarlos de manera incompatible con las finalidades de esa

[193] Vid. Sentencia del Tribunal de Justicia de la Unión Europea, de 6 de octubre de 2015, en el asunto C-362/14, fragmento número 88.
[194] Vid. Sentencia del Tribunal de Justicia de la Unión Europea, de 6 de octubre de 2015, en el asunto C-362/14, fragmento número 89.

transferencia, que va más allá de lo que era estrictamente necesario y proporcionado para la protección de la seguridad nacional[195].

Por último, puesto que la adopción por la Comisión de una decisión en virtud del artículo 25.6 de la Directiva 95/46/CE requería la constatación debidamente motivada por esa institución de que el tercer país considerado –en este caso, EE.UU.- garantizaba efectivamente, por su legislación interna o sus compromisos internacionales, un nivel de protección de los derechos fundamentales sustancialmente equivalente[196], la inexistencia de este presupuesto esencial vulneraba la exigencia del artículo 25.6 de la Directiva.

3. Consecuencias de la Sentencia del TJUE de 6 de octubre de 2015.

Tras la publicación de esta Sentencia, el Grupo de Trabajo del Artículo el 16 de octubre de 2015[197] emitió una nota de prensa en la que señalaba la necesidad de contar con una "posición sólida, colectiva y común sobre la aplicación de la sentencia" , haciendo un llamamiento urgente a los Estados miembros y a las instituciones europeas para iniciar las conversaciones con las autoridades de Estados Unidos a fin de "encontrar soluciones políticas, jurídicas y técnicas que permitan transferencias de datos a Estados Unidos", respetando los derechos fundamentales, todo ello mediante "mecanismos claros y vinculantes" [198]. También, el Grupo de Trabajo del Artículo 29

[195] Ello lo constató la Comisión en los puntos 2 y 3.2 de la Comunicación COM (2013) 846 final y en los puntos 7.1, 7.2 y 8 de la Comunicación COM (2013) 847 final.

[196] Vid. Sentencia del Tribunal de Justicia de la Unión Europea, de 6 de octubre de 2015, en el asunto C-362/14, fragmento número 96.

[197] Como señala HERNANDEZ MUÑOZ, tras la sentencia se ha creado una "situación de enorme inseguridad, pues nadie sabe cómo se van a regular finalmente estas transferencias, siendo demasiadas las preguntas sin respuesta: ¿se va a exigir el procedimiento ordinario de solicitud de autorización de trasferencias internacionales cuando se destinen a cualquier empresa de EE.UU., esté o no adherida a los principios *safe harbor?*, ¿se van a realizar labores de inspección a todas las transferencias internacionales realizadas a empresas *safe harbor?*, ¿qué va a pasar con las denominadas «Cláusulas Contractuales Tipo y Normas Corporativas Vinculantes» entre empresas?, ¿se va a exigir que todos aquellos que hayan transferido datos a estas empresas regularicen su situación iniciando un procedimiento ordinario de solicitud de autorización?, ¿se va a regular un nuevo procedimiento especial?, ¿cuál va a ser, en su caso, el plazo establecido para realizar la regularización?, ¿a partir de ahora, qué tienen que hacer las empresas de la UE que vayan a transferir datos personales a empresas norteamericanas *safe harbor* hasta que los órganos de control europeos fijen las líneas comunes de actuación? HERNÁNDEZ MUÑOZ, Reyes, Ataque al safe harbor. Contundente ofensiva europea contra efectivos estadounidenses en materia de protección de datos, Diario La Ley, nº 8655, 2015, p. 2.

[198] "Following the landmark ruling of the Court of Justice of the European Union (CJEU) of 6 October 2015 in the Maximilian Schrems v Data Protection Commissioner case (C-362- 14), the EU data protection authorities assembled in the Article 29 Working Party have discussed the first consequences to be drawn at European and national level. EU data protection authorities consider that it is absolutely

deja claro y sin ningún género de dudas que, tras la sentencia, las transferencias procedentes de la UE que aún se estén llevando a cabo bajo la Decisión de 26 de julio de 2000 son ilegales[199].

Con posterioridad, el día 29 de octubre la Agencia Española de Protección de Datos envió una comunicación a todas las empresas que utilizaban el Puerto Seguro para la realización de transferencias internacionales, poniendo a su servicio canales de información adecuados[200].

De acuerdo con la comunicación de la AEPD sobre la aplicación de la sentencia de Puerto Seguro[201] los responsables del tratamiento debían informar al Registro General de Protección de Datos de la AEPD antes de finales de enero de 2016 sobre la continuidad de las transferencias y sobre su adecuación a la normativa de protección de datos. Hay que mencionar, además, que la AEPD anunció que no tenía intención de iniciar procedimientos sancionadores por defecto contra las empresas, pero apercibió a los responsables que, de no modificarse la base legal para la realización de transferencias, la Agencia podría iniciar el procedimiento para acordar la suspensión temporal de las transferencias.

---

essential to have a robust, collective and common position on the implementation of the judgment. Moreover, the Working Party will observe closely the developments of the pending procedures before the Irish High Court". Statement of the Article 29 Working Party, 16 de octubre de 2015, en línea: 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 10.04.2016].

[199] Vid. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, 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: 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 25 de octubre de 2015].

[200] Vid. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Comunicación enviada a responsables, 29 de octubre de 2015, en línea: https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/common/Comunicacion_responsables_-_Puerto_Seguro.pdf [consultado el 2 de noviembre de 2015].

[201] Vid. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Nueva comunicación sobre la aplicación de la sentencia de Puerto Seguro, en línea: https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/AplicacionSentenciaSH-ides-idphp.php [consultado el 20.11.2015].

V. EL NUEVO ACUERDO *EU-US PRIVACY SHIELD.*

El 2 de febrero de 2016 la Comisión Europea y los Estados Unidos de América anunciaron su voluntad[202] de entablar un acuerdo que crease un nuevo marco regulador de las transferencias internacionales de datos entre la UE y los EE UU, que se convertiría en sucesor de Declaración de Puerto Seguro, invalidada por el Tribunal de Justicia de la Unión Europea[203].

A continuación se expondrá brevemente los aspectos más novedosos del nuevo acuerdo, denominado *EU-US Privacy Shield*, para evaluar si refleja los requerimientos efectuados por el Tribunal de Justicia de la Unión Europea en la Sentencia de 6 de octubre de 2015.

En primer término, conviene remarcar que, mediante este acuerdo, Estados Unidos se comprometería, por primera vez, a establecer garantías, limitaciones y mecanismos de supervisión en relación con el acceso por las autoridades públicas estadounidenses a los datos personales transferidos desde la UE para la aplicación de la ley y la seguridad nacional estadounidense, apuntando que "*these exceptions must be used only to the extent necessary and proportionate*"[204]. En particular, EEUU ha descartado la realización de actividades de vigilancia masiva indiscriminada de los datos personales transferidos a los EEUU, y todo ello se controlaría mediante una revisión conjunta anual efectuada por la Comisión y el Departamento de Comercio de los EEUU, a la cual se hallarían invitados expertos de inteligencia de los EEUU y autoridades europeas de protección de datos.

---

[202] "The College has today mandated Vice-President **Ansip** and Commissioner **Jourová** to prepare a draft "adequacy decision" in the coming weeks, which could then be adopted by the College after obtaining the advice of the Article 29 Working Party and after consulting a committee composed of representatives of the Member States. In the meantime, the U.S. side will make the necessary preparations to put in place the new framework, monitoring mechanisms and new Ombudsman". EUROPEAN COMMISSION. PRESS RELEASE, EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield, 2 february 2016, en línea: http://europa.eu/rapid/press-release_IP-16-216_en.htm [consultado el 4.02.2016].

[203] Vid. AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, La Comisión Europea y EEUU anuncian un acuerdo para la realización de transferencias internacionales de datos, en línea: https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2016/notas_prensa/news/2016_02_03-ides-idphp.php [consultado el 5.02.2016].

[204] Vid. EUROPEAN COMMISSION. PRESS RELEASE, EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield, 2 february 2016, en línea: http://europa.eu/rapid/press-release_IP-16-216_en.htm [consultado el 4. 02.2016].

En segundo lugar, en el ámbito de la tutela judicial efectiva es novedosa la imposición de plazos a las empresas para responder a las quejas efectuadas por los particulares, así como la eliminación de los costes por acudir a los mecanismos de resolución alternativa de los conflictos, servicios que pasarían a ser gratuitos.

A ello cabe añadir que, mediante el nuevo acuerdo, las agencias europeas de protección de datos podrían derivar las quejas de los particulares al Departamento de Comercio y a la Comisión Federal de Comercio y, en el ámbito del acceso por las autoridades de inteligencia estadounidenses a los datos personales transmitidos desde la UE, se crearía un nuevo Defensor especializado en esta materia.

No obstante, a pesar del novedoso contenido de este acuerdo, se puede apreciar que no atiende al requerimiento principal efectuado por el TJUE en su Sentencia de 6 de octubre de 2016, según el cual la protección adecuada de los datos debe otorgarla el ordenamiento jurídico de EE.UU en razón de su "legislación interna y compromisos internacionales".

VI. ANÁLISIS DE LA POLÍTICA DE DATOS DE FACEBOOK.

Dado que Facebook es una de las redes más usadas por los internautas españoles[205], a continuación se efectuará un estudio de la Política de datos de la red social Facebook, analizando, en primer término, qué tipo de información recopila sobre los usuarios del servicio y durante cuánto tiempo la conserva; en segundo lugar, se constatará cuál es el uso que le da a la información recogida y, en concreto, si el mismo incluye la cesión de los datos a terceros. En tercer lugar, se hará especial referencia al régimen que, en la actualidad, utiliza Facebook con respecto a las transferencias internacionales de datos efectuadas desde la Unión Europea. Por último, se detallarán cuáles son las previsiones de Derecho Internacional Privado que se prevén en la "Declaración de derechos y responsabilidades" de los Principios de Facebook, en particular, la determinación de la competencia judicial internacional y del derecho aplicable.

[205] Vid. Online Business School presenta el estudio **Social Media 2015**, que analiza las tendencias de uso y participación en redes sociales tanto en España como en las principales economías mundiales, en línea: http://www.obs-edu.com/noticias/estudio-obs/espana-aumenta-el-numero-de-usuarios-activos-en-redes-sociales-en-2014-y-llega-los-17-millones/ [consultado el 10.12.2015].

Deseo subrayar, en primer término, que Facebook Inc. recopila toda la información que el usuario proporciona cuando utiliza sus servicios, tanto el "contenido" como "otros datos" relacionados con éste.

A título ilustrativo, conviene remarcar que Facebook recopila el contenido que el usuario comparte públicamente, así como el contenido de los mensajes "privados" que el usuario envía a otros usuarios. En cuanto a los datos relacionados con el contenido, Facebook conserva datos tales como el lugar dónde se realizan las fotos, la fecha de creación de los archivos, e información acerca de los "ordenadores, teléfonos u otros dispositivos" desde los que el usuario accede a los servicios.

También, cabe destacar que esta red social recopila información sobre las personas y los grupos a los que se halla conectado el usuario, y sobre el modo de interactuar con los mismos –por ejemplo, recopila cuáles son las personas o grupos con los que más se comunica el usuario-, así como la información relacionada con los sitios web que visita el usuario y que utilizan los servicios de Facebook, bien ofreciendo el botón "Me gusta", bien haciendo uso de los servicios de "medición y publicidad".

Además, que si se utilizan los servicios de Facebook para efectuar compras o transacciones financieras, esta compañía recopila los datos que envuelven a la transacción en cuestión, incluyendo los "datos de pago, como el número de tarjeta de crédito o débito (…), además de información e facturación, envío y contacto".

Si bien el principio de calidad de los datos exige que los datos personales no deben ser conservados "*en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados*"[206], Facebook almacena los datos "durante el tiempo necesario para facilitar productos y servicios a los usuarios", conservando la información asociada a una cuenta hasta que la misma se elimine, a menos que dicha compañía "ya no necesite los datos para ofrecer los productos y servicios".

En cuanto al uso que Facebook da a la información recogida se define de forma abstracta. Así, la entidad señala que usa "toda la información de la que disponemos", es decir, independientemente de si la misma se refiere a datos de carácter sensible o no, para "personalizar el contenido y proponerte sugerencias", "ofrecerte accesos directos",

[206] Vid. Artículo 4.5 de la LOPD.

"adaptar nuestros servicios a tus necesidades y a las de otros usuarios" para "enviarte mensajes de marketing", para "mejorar nuestros sistemas de publicidad y medición con el fin de mostrarte anuncios relevantes", entre otros aspectos.

Conviene añadir que Facebook efectúa cesiones de datos personales a dos tipos de "colaboradores externos". Por una parte, la entidad comparte "toda la información" que posee sobre los usuarios a los "servicios de publicidad, medición y análisis" con el objetivo de mostrarles anuncios relevantes, sin que se ceda la información que permita identificar a la persona, a menos que el usuario de permiso expreso.

Por otra parte, Facebook transfiere información a "proveedores, proveedores de servicios y a otros socios de todo el mundo que nos ayudan a mantener nuestro negocio prestando servicios de infraestructura técnica, analizando el uso que se hace de nuestros servicios, midiendo la eficacia de los anuncios y servicios, realizando investigaciones académicas (…)", etcétera. En este supuesto, la compañía suscribe un contrato, mediante el cual el cesionario debe cumplir "estrictas obligaciones de confidencialidad". No obstante, en este segundo supuesto la información que se comparte sí que puede identificar a la persona física –motivo por el cual entran en la definición de "datos personales"-, y el interesado no goza de mecanismo alguno para controlar el uso que estos "proveedores, proveedores de servicios y a otros socios de todo el mundo" están dando a los datos en cuestión. Así, Facebook puede compartir información "por vías internas en el seno de su grupo de empresas" o "con terceros", pudiendo transferirse la información recopilada en el EEE a países de fuera del EEE a los efectos descritos su política de datos.

En este sentido, es relevante la previsión según la cual Facebook puede "consultar, procesar o conservar" la información que reciba sobre los usuarios "durante un período prolongado de tiempo cuando esté sujeta a una solicitud u obligación judicial, una investigación gubernamental o investigaciones relacionadas con posibles infracciones de nuestras políticas o condiciones, o bien para evitar daños", y ello porque legitima la vigilancia masiva de los ciudadanos usuarios de Facebook por parte del Gobierno de los Estados Unidos.

En tercer lugar, deseo remarcar que Facebook todavía no ha actualizado su régimen en relación a las transferencias internacionales de datos personales pues, al tenor de su Política de datos, éste "cumple el marco *Safe Harbor* entre Estados Unidos y la Unión

Europea y entre Estados Unidos y Suiza con relación a la recopilación, el uso y la retención de datos pertenecientes a la Unión Europea y Suiza, según lo dispuesto por el Departamento de Comercio de Estados Unidos" [207]. Además, se añade que los conflictos que puedan surgir en relación con sus políticas y prácticas pueden resolverse a través de *TRUSTe*[208], mecanismo alternativo de resolución de conflictos previsto en el Anexo II de la Decisión de la Comisión de 26 de julio de 2000, invalidada por la STJUE de 6 de octubre de 2015.

Sin embargo, en la Cláusula 16 de la "Declaración de derechos y responsabilidades", también denominada "Condiciones", se prevén un conjunto de "*Disposiciones especiales aplicables a usuarios que no residan en Estados Unidos*" cuyo apartado primero prevé que el usuario da su consentimiento[209] para que sus datos personales sean transferidos y procesados en Estados Unidos. Si esta previsión podía ser válida al tenor del artículo 26.1 a) de la Directiva 95/46/CE, ahora la excepción del artículo 49.1 a) del nuevo Reglamento exige que, además de que el interesado haya dado explícitamente su consentimiento a la transferencia propuesta, que el mismo 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.

Por último, del análisis de la "Declaración de derechos y responsabilidades" que tiene origen en los Principios de Facebook cabe remarcar la previsión contenida en la Cláusula 15, que prevé los tribunales que gozan de competencia judicial internacional, así como el derecho que resultaría aplicable en el supuesto de litigio relacionado con Facebook. En virtud de dicha cláusula el usuario acepta que únicamente el tribunal del Distrito de California o un tribunal estatal del Condado de San Mateo, sean los competentes a la hora de resolver los litigios de dichos conflictos. En lo que al derecho aplicable se refiere, se añade que "las leyes del estado de California rigen esta Declaración, así como cualquier demanda que pueda surgir entre tú y nosotros".

---

[207] Vid. US-EU SAFE HARBOUR LIST, en línea: https://safeharbor.export.gov/list.aspx [25.04.2016].
[208] Vid. TRUSTe Feedback and Resolution System, en línea: https://feedback-form.truste.com/watchdog/request [consultado el 25.04.2016].
[209] Como señala DAVARA RODRÍGUEZ, si bien haciendo referencia a los términos y condiciones del servicio Whatsapp, "el propio usuario se muestra despreocupado aceptando términos y condiciones de uso en los que él mismo está otorgando el consentimiento para el tratamiento y, en su caso, cesión de datos a terceros". DAVARA RODRÍGUEZ, Miguel Ángel, "Intercambio de mensajes por Internet: el caso Whatsapp", *El Consultor de los Ayuntamientos: Revista técnica especializada en administración local y justicia*, nº 7, (2014), p. 834.

CONCLUSIONES

Como resultado del análisis que se ha venido efectuando a lo largo del presente Trabajo de Final de Grado puedo concluir que, mediante la regulación de las transferencias internacionales de datos, la UE y, en particular, el ordenamiento jurídico español, pretenden hacer valer el derecho fundamental a la protección de los datos personales, con el propósito de impedir que el tráfico ilícito de los mismos lesione la dignidad de los sujetos afectados. Dado que nos hallamos insertos en la globalización tecnológica, he podido constatar que las transferencias de los datos personales desde un Estado miembro de la UE que los protege como derechos fundamentales hacia otro que no ofrece tales garantías supone, en ocasiones, la pérdida de control de los mismos por parte de sus titulares y la ineficacia de la normativa protectora del Estado miembro de la UE desde el cual se exportan.

A lo largo del Capítulo III se ha examinado el sistema por el cual la UE, mediante la Directiva 95/46/CE, ha pretendido hacer valer los derechos ligados a la protección de los datos personales cuando los mismos se transmiten a países terceros, no miembros de la Unión. La regla general es que se hallan prohibidas las transferencias internacionales de datos cuando el tercer país no garantiza una protección adecuada de los derechos fundamentales de los sujetos afectados, situación que es analizada por la Comisión a la vista de su "*legislación interna o compromisos internacionales*", emitiendo la correspondiente Decisión. Como se ha apuntado a lo largo del Trabajo, este tipo de transferencias gozan del beneficio de no requerir garantías adicionales por parte de los sujetos que las llevan a cabo. Por otra parte, se ha verificado que es posible efectuar transferencias internacionales de datos a países que no aportan un nivel adecuado de protección de los datos personales, cuando el responsable del tratamiento ha aportado "garantías adecuadas" y obtenido la correspondiente autorización por parte de la Agencia de Protección de Datos –cabiendo entender por "garantías adecuadas", tanto la suscripción de contratos-tipo aprobados por la Comisión o la Agencia, como de normas corporativas vinculantes, entre el importador y el exportador de los datos personales-.

Se ha evidenciado cómo la regulación de las transferencias internacionales de datos pretende ponderar los dos intereses jurídicos en juego, por una parte, no impedir los flujos transfronterizos de datos personales, que son necesarios para la expansión del

comercio y, por otra parte, la protección de las personas físicas en lo que a sus datos personales se refiere.

No obstante, para la UE alcanzar el objetivo mencionado ha significado y deviene todo un reto cuando, por una parte, el "tercer país" que actúa como importador de los datos personales transferidos desde la UE es Estados Unidos de América, cuyo sistema interno de protección de los datos personales no sólo difiere sustancialmente del previsto en la UE, sino que, además, legitima a sus autoridades el acceso masivo a los datos almacenados y tratados en su territorio.

A pesar de su patente condición de "tercer país" que no garantiza un "nivel de protección adecuado" de los datos personales, los grandes intereses políticos y económicos de ambas potencias llevaron a la Comisión Europea a emitir la Decisión de 26 de julio de 2000, por la que se creó el sistema de adhesión voluntaria a los Principios de Puerto Seguro y a sus correspondientes Preguntas más Frecuentes. Este sistema pretendía dar una respuesta compatible con los intereses de la industria norteamericana, la cual tan sólo había limitado su derecho al uso de los datos personales mediante la autorregulación o *self-regulation* y, al mismo tiempo, facilitar el flujo transatlántico de datos, asumiendo las entidades adheridas al mismo el estatuto de tercer país que garantiza un nivel de protección adecuado de los datos, sin que sea necesaria garantía ni autorización adicional alguna.

Del análisis crítico de la Decisión de la Comisión de 26 de julio de 2000 he podido concluir que su contenido, no sólo se aleja de una protección "equiparable" a la que confiere la UE, sino que además presenta ciertos vicios que justifican su posterior anulación por parte del TJUE en su Sentencia de 6 de octubre de 2015. En primer término, es una Decisión que no se ajusta a lo dispuesto en el artículo 25.6 de la Directiva 95/46/CE, pues la misma no declara que el ordenamiento jurídico de EE.UU, como "tercer país", garantice un nivel adecuado de protección, sino que tan sólo las entidades que se adhieran a los Principios y las FAQ que la misma contiene adquieren el estatuto de "país tercero que garantiza un nivel de protección adecuado".

En segunda instancia, he podido constatar que desde el año 2000 al 2009 el Departamento de Comercio de EE.UU no ha efectuado control previo alguno de las políticas de privacidad presentadas por las entidades que pretendían adherirse al régimen de Puerto Seguro, motivo por el cual las entidades norteamericanas adheridas

al mismo podían recibir libremente datos procedentes de la Unión Europea, pues formalmente estaban adheridas al acuerdo de Puerto Seguro, pero en realidad podían violar manifiestamente los derechos fundamentales de los titulares de los datos, pues ninguna autoridad había constatado que sus políticas cumpliesen con lo dispuesto en el acuerdo. Con posterioridad, y como respuesta a las peticiones de la Comisión, el Departamento comenzó a efectuar "controles formales" de las nuevas solicitudes de adhesión a los Principios que, como su denominación indica, no conllevaban el análisis de las prácticas o conductas reales de las entidades. Además, cabe cuestionar la rigidez de estos controles formales pues, como se ha podido ver, tan sólo un 12% de las entidades que solicitaron la adhesión en 2013 no fueron incluidas en la lista.

A ello debe añadirse que, durante el período de tiempo en que las entidades se han hallado adheridas al régimen de Puerto Seguro, los controles periódicos de cumplimiento se han basado principalmente en el procedimiento de "autoevaluación", pues "verificación por terceros" era una opción voluntaria. Por todo lo expuesto, una entidad que violase manifiestamente los derechos fundamentales de los titulares de los datos transmitidos desde la UE podía persistir en su incumplimiento sin resultar percibida hasta que un particular decidiese interponer la correspondiente denuncia.

En tercer lugar, dado que la Decisión de la Comisión de 26 de julio de 2000 no declaró que el ordenamiento jurídico de EE.UU garantizase de forma adecuada los datos personales, las leyes y la jurisprudencia aplicables en dicho país no sólo han venido vulnerando el régimen de Puerto Seguro sino que, además han gozado de primacía con respecto a dicho acuerdo, pues el mismo preveía que la adhesión podía limitarse para cumplir exigencias de seguridad nacional, interés público y cumplimiento de la ley estadounidense, sin que exigiese a las autoridades públicas estadounidenses su sumisión a los principios.

Debe remarcarse, en cuarto lugar, que la determinación de los sectores excluidos e incluidos en el ámbito de aplicación de la Decisión tiene un marcado carácter ambiguo. Si bien no se establece de forma directa los sectores que no pueden adherirse al acuerdo de Puerto Seguro, ello si se hace de forma indirecta, al establecer límites a las competencias de los organismos públicos que asumen la función de controlar a las entidades adheridas, resolviendo los recursos que impongan los particulares y, en su caso, sancionando a las compañías incumplidoras. Así, la FTC tan sólo tiene

competencia en los actos desleales y engañosos que tengan lugar en el "ámbito del comercio" y carece de jurisdicción "en lo tocante a bancos, cooperativas de ahorro y crédito, compañías de servicio público de telecomunicaciones y de transporte, compañías aéreas y envasadores y operarios de áreas para el ganado" y el Departamento de Transporte de EE.UU goza de competencia con respecto a "agentes de viajes, compañías aéreas, organismos públicos estadounidenses y extranjeros". Estos límites también se aprecian en los órganos de ADR que prevé el régimen de Puerto Seguro, que cubren tan sólo las actividades "online".

En quinto lugar, y ateniendo a un aspecto más sustantivo del régimen de Puerto Seguro se ha podido analizar cómo derechos tan esenciales como los derechos de opción, de acceso y de notificación se hallaban sumamente limitados, estipulando sus excepciones de manera muy abstracta y haciendo un uso excesivo de conceptos jurídicos indeterminados. Baste recordar que se podía exigir una cuota a los particulares que pretendiesen ejercer su derecho de acceso, así como la entidad podía rechazar dicho acceso alegando una "carga o dispendio desproporcionado". Además, no se prevé control alguno para las transferencias ulteriores de los datos personales que puedan efectuar las entidades adheridas al acuerdo de Puerto Seguro, pues tan sólo se exige el cumplimiento de los principios de notificación y opción –que igualmente se hallan restringidos-, y la suscripción de un "convenio" que ofrezca el nivel de protección de los principios, sin que ninguna autoridad controle el contenido del convenio en cuestión. Por lo tanto, si ya el particular ha tenido dificultades para ejercer sus derechos ante entidades certificadas, la transmisión de los datos a terceros por parte de las mismas supone una imposibilidad casi total de ejercer sus derechos fundamentales.

Además de la falta de transparencia y de control en la ejecución del régimen de puerto seguro, el principal problema que cabe esgrimir con respecto a su efectiva aplicación es que aproximadamente todas las empresas involucradas en programas de espionaje masivo como el programa PRISM, y que han venido concediendo a las autoridades estadounidenses acceso a los datos almacenados y tratados en EE.UU, se hallaban adheridas al régimen de Puerto Seguro. Como se ha estudiado a lo largo del Trabajo, si bien suele alegarse por parte del Gobierno de EE.UU que los registros de "metadatos" no incluyen información alguna sobre el contenido de las comunicaciones, ya se ha evidenciado cómo los "metadatos" permiten analizar grandes conjuntos de datos para identificar hábitos y comportamientos de personas físicas identificadas, motivo por el

cual son merecedores de protección, por subsumirse en la definición de "datos personales".

En vista de los argumentos esgrimidos por el TJUE para anular la Decisión de la Comisión, he podido verificar que el *EU-US Privacy Shield* no atiende al requerimiento principal efectuado por el TJUE en su Sentencia de 6 de octubre de 2016, según el cual la protección adecuada de los datos debe otorgarla el ordenamiento jurídico de EE.UU en razón de su "*legislación interna y compromisos internacionales*".

Por último, deseo subrayar que la aprobación el Reglamento (UE) 2016/679 del Parlamento y del Consejo, de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, que ha derogado la Directiva 95/46/CE, supondrá un cambio sustancial en lo que al régimen de las transferencias internacionales de datos se refiere. Baste mencionar, como muestra, que las decisiones de adecuación de la Comisión Europea podrán referirse tanto a un *"tercer país*" u "*organización internacional*", como a un "*territorio*" o a "*uno o varios sectores específicos de ese tercer país*", para la lo cual esta Institución deberá atender a unos criterios más específicos, en concreto, a "*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*".

Hallándonos en el inicio de la nueva "era digital", en que los datos personales se están convirtiendo en un activo de gran valor –ya se apuntó que el valor estimado de los datos de los ciudadanos de la UE fue de 315 000 millones de euros en 2011 y tiene un potencial de crecimiento de casi 1 billón de euros al año hasta 2020-, se ha podido constatar cómo la UE pretende imponer a los terceros países que pretendan recibir datos personales desde la misma su propia concepción del derecho a la protección de los datos personales, objetivo cuyo cumplimiento se hace progresivamente más dificultoso, atendiendo a los nuevos retos que plantea la nueva era del "imperialismo digital".

BIBLIOGRAFÍA

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *El derecho fundamental a la protección de datos: guía para el ciudadano*, 2011.

ARRIBAS LUQUE, José María, "Sobre la protección adecuada en las transmisiones de datos personales desde la Unión Europea a los EE.UU.: El sistema de principios de Puerto Seguro", *Diario La Ley*, nº 549, (2002), pág. 1-24.

BALERO TORRIJOS, Julián, *La Protección de los Datos Personales en Internet ante la Innovación Tecnológica*, Ed. Thomson Reuters Aranzadi, Navarra, 2013.

BRU CUADRADA, Elisenda, "La protección de datos en España y en la Unión Europea. Especial referencia a los mecanismos jurídicos de reacción frente a la vulneración del derecho a la intimidad", *Revista de Estudios de Derecho y Ciencia Política de la UOC*, nº 5, (2007), págs. 78-92.

CÁRDENAS ARTOLA, Ignacio; FERRERO RECASENS, Eduardo, entre otros, *Memento experto. Protección de datos*, Ed. Francis Lefebvre, Madrid, 2012.

DURÁN CARDO, Ana Belén, *La figura del responsable en el derecho a la protección de datos. Génesis y evolución normativa ante el cambio tecnológico y en perspectiva multinivel*, Universidad Autónoma de Barcelona, Barcelona, 2015.

DAVARA RODRÍGUEZ, Miguel Ángel, "Intercambio de mensajes por Internet: el caso Whatsapp", *El Consultor de los Ayuntamientos: Revista técnica especializada en administración local y justicia*, nº 7, (2014), págs. 832-837.

DE MIGUEL ASENSIO, Pedro Alberto, *Protección de datos personales*, Ed Aranzadi, Madrid.

GUASCH PORTAS, Vicente, *Las transferencias internacionales de datos en la normativa española y comunitaria*, Agencia Española de Protección de Datos y Agencia Estatal Boletín Oficial del Estado, Madrid, 2014.

GUASCH PORTAS, Vicente, "La transferencia internacional de datos de carácter personal", *Revista de Derecho UNED*, núm. 11, (2012), págs. 413-453.

HERNÁNDEZ MUÑOZ, Reyes, "Ataque al safe harbor. Contundente ofensiva europea contra efectivos estadounidenses en materia de protección de datos", *Diario La Ley*, nº 8655, (2015), pág. 1-3.

HOLVAST, Jan, "History of Privacy", en DE LEEUW, Karl y BERGSTRA, Jan (eds.) *The History of Information Security: A Comprehensive Handbook,* Ed. Elsevier, Ámsterdam, 2007.

J. SOLOVE, Daniel, "A Brief History of Information Privacy Law", en DANIEL J. SOLOVE, MARC ROTENBERG Y PAUL M. SCHWARTZ, *Information Privacy Law*, Ed. Wolters Kluwer, New York, 2006.

MARZO PORTERA, Ana; ORTEGA GIMÉNEZ, Alfonso, *Empresa y transferencia internacional de datos personales*, ICEX (Instituto Español de Comercio Exterior), Madrid, 2013.

ORTEGA GIMÉNEZ, Alfonso, *La (des)protección del titular del derecho a la protección de datos derivada de una transferencia internacional ilícita*, Agencia Española de Protección de datos, Madrid, 2014.

ORTEGA GIMÉNEZ, Alfonso, "Internet, publicación de datos personales y transferencias internacionales de datos: la sentencia del TJCE "Lindqvist", de 6 de noviembre de 2003, Aranzadi Bibliotecas, 2009.

REBOLLO DELGADO, Lucrecio, *Manual de protección de datos,* Ed. Dykinson, Madrid, 2014.

REDACCIÓN DIARIO LA LEY, "Las explicaciones de EE.UU. sobre el programa de espionaje masivo no convencen a la UE", *Diario La Ley*, nº 8175, (2013), pág. 1-2.

REIDENBERG, Joel R.; RUSSELL, N. Cameron, entre otros, *Privacy and Cloud Computing in Public Schools*, Center on Law and Information Policy, 2013.

SANCHO VILLA, Diana, *Transferencia internacional de datos personales,* Agencia de Protección de Datos, Madrid, 2003.

SANCHO VILLA, Diana, "Protección de los datos personales y transferencia internacional: cuestiones de ley aplicable", *Revista Jurídica de Castilla y León*, nº 16, (2008), págs. 401-445.

ZUFIAUR NARVAIZA, José María, "Globalización económica y deslocalizaciones productivas", *Relaciones laborales: Revista crítica de teoría y práctica*, nº 1, (2005), págs. 1157-1176.

JURISPRUDENCIA

Sentencia del Tribunal Constitucional núm. 254/1993, de 20 de julio (Rec. 1827/1990).

Sentencia del Tribunal Constitucional núm. 292/2000, de 30 de noviembre (Rec. 1463/2000).

Sentencia del Tribunal de Justicia de las Comunidades Europeas, de 6 de noviembre de 2003, Caso Proceso penal contra Bodil Lindqvist (TJCE 2003\368).

Sentencia del Tribunal de Justicia de la Unión Europea, de 6 de octubre de 2015, en el asunto C-362/14, que tiene por objeto una petición 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 Data Protection Commissioner.

Memorandum opinion of United States District Court for the District of Columbia, de 16 de diciembre de 2013 (Civil Action No. 13-0851).

DOCUMENTOS DEL GRUPO DE TRABAJO DEL ARTÍCULO 29 Y DE LA COMISIÓN EUROPEA.

Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Comission and the United States Government, adopted by the Working Party on 26 January 1999 (5092/98/EN/final WP 15).

Opinion 2/99 on the Adequacy of the "International Safe Harbor Principles" isued by the US Department of Commerce on 19th April 1999, adopte don 2 May 1999 (5047/99/EN/final WP 19).

Opinion 4/99 on The Frequently Asked Questions to be issued by the US Department of Commerce in relation to the proposed “Safe Harbor Principles”, adopte don 7 June 1999 (5066/99/EN/final WP 21).

Working document on the current state of play of the ongoing discussions between the European Comission and the United States Government concerning the “International Safe Harbor Principles”, adopte don 7 July 1999 (5075/99/EN/final WP 23).

Opinion 7/99 on the Level of Data Protection provided by the “Safe Harbor” Principles as published together with the Frequently Asked Questions (FAQs) and other related documents on 15 and 116 November 1999 by the US Department of Commerce, adopted on 3 December 1999 (5146/99/EN/final WP 27).

Opinion 3/200 on the EU/US dialogue concerning the “Safe Harbor” arrangement, adopte don 16th March 2000 (5019/00/EN/FINAL WP 31).

Opinion 4/2000 on the level of protection provided by the “Safe Harbor Principles”, adopte don 16th May 2000 (CA07/434/00/EN WP 32).

Working Document on Functioning of the Safe Harbor Agreement, adopte don 2 July 2002 (11194/02/EN WP 62).

Resolución del Parlamento Europeo sobre el proyecto de decisión de la Comisión relativa a la adecuación de la protección garantizada por los principios estadounidenses de puerto seguro y preguntas más frecuentes relacionadas publicadas por el Departamento de Comercio de los EE.UU. (C5-0280/2000 – 2000/2144 COS),

Dictamen 04/2014 del Grupo de Trabajo del Artículo 29, sobre la vigilancia de las comunicaciones a efectos de inteligencia y seguridad nacional, adoptado el 10 de abril de 2014 (819/14/EN WP 215)

Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE, de 27 de noviembre de 2013, COM (2013) 847 final.

Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre restablecer la confianza en los flujos de datos entre la UE y EE.UU, de 27 de noviembre de 2013. COM (2013) 846 final.

WEBGRAFÍA

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, 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: 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 25 de octubre de 2015].

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Comunicación enviada a responsables, 29 de octubre de 2015, en línea: https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/common/Comunicacion_responsables_-_Puerto_Seguro.pdf [consultado el 2 de noviembre de 2015]

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Nueva comunicación sobre la aplicación de la sentencia de Puerto Seguro, en línea: https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/AplicacionSentenciaSH-ides-idphp.php [consultado el 20.11.2015].

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Inscripción de ficheros, en línea: https://www.agpd.es/portalwebAGPD/canalresponsable/inscripcion_ficheros/index-ides-idphp.php [consultado el 29.02.2016].

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, La Comisión Europea y EEUU anuncian un acuerdo para la realización de transferencias internacionales de datos, en línea: https://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2016/notas_prensa/news/2016_02_03-ides-idphp.php [consultado el 5.02.2016].

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *Transferencias internacionales de datos*, Autorización de la Directora de la Agencia Española de Protección de Datos, en línea:

https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/index-ides-idphp.php [consultado el 1.03.2016].

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, *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 18.03.2016].

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, Elaboración de Códigos Tipo. Objeto y naturaleza, en línea: https://www.agpd.es/portalwebAGPD/canalresponsable/elaboracion_codigos_tipo/index-ides-idphp.php [consultado el 16.03.2016].

ARTICLE 29 WORKING PARTY, Statement of 16 de octubre de 2015, en línea: 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 10.04.2016].

CONSTITUTION OF THE UNITED STATES OF AMERICA: Analysis and Interpretation, en línea: https://www.congress.gov/constitution-annotated/ [consultado el 16.03.2016].

EUROPEAN COMMISSION. PRESS RELEASE, EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield, 2 february 2016, en línea: http://europa.eu/rapid/press-release_IP-16-216_en.htm [consultado el 4. 02.2016].

EL MUNDO, El Senado de EEUU aprueba la nueva Ley de Escuchas Telefónicas, 10 de julio de 2008, en línea:

http://www.elmundo.es/elmundo/2008/07/10/internacional/1215647473.html [consultado el 15.04.2016].

EL MUNDO, EEUU "espía" a través de los servidores de Apple, Google o Facebook, 7 de junio de 2013, en línea:

http://www.elmundo.es/america/2013/06/07/estados_unidos/1370577062.html [consultado el 20.04.2016].

EL PAÍS, Imperialismo digital, EEUU usa la información para proteger su economía y el éxito depende de la pasividad de sus víctimas, 1 de noviembre de 2013, en línea: http://internacional.elpais.com/internacional/2013/11/01/actualidad/1383333227_605243.html [consultado el 1.05.2016].

FURNISH, Dale Beck, *Fuentes del Derecho en Estados Unidos. La muerte del derecho consuetudinario. Las fuentes escritas en la edad del derecho positivo, y el papel y efecto de los Restatements of the law*, en línea: http://www.juridicas.unam.mx/publica/librev/rev/facdermx/cont/235/art/art3.pdf [consultado 10.12.2015].

HARVARD LAW REVIEW, commentary by Charles E. Colman, en línea: http://harvardlawreview.org/2016/01/about-ned/ [consultado el 25.03.2016].

ONLINE BUSINESS SCHOOL, estudio Social Media 2015, en línea: http://www.obs-edu.com/noticias/estudio-obs/espana-aumenta-el-numero-de-usuarios-activos-en-redes-sociales-en-2014-y-llega-los-17-millones/ [consultado el 10.12.2015].

THE GUARDIAN, *NSA Prism program taps in to user data of Apple, Google and others*, 6 de junio de 2013, en línea: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data [consultado el 03.04.2016].

THE FOURTH AMENDMENT: Search and seizure, en línea: https://www.congress.gov/content/conan/pdf/GPO-CONAN-REV-2014-10-5.pdf [consultado el 16.03.2016].

THE FIFTH AMENDMENT: Rights of persons, en línea: https://www.congress.gov/content/conan/pdf/GPO-CONAN-REV-2014-10-6.pdf [consultado el 16.03.2016].

TRUSTe, Feedback and Resolution System, en línea: https://feedback-form.truste.com/watchdog/request [consultado el 25.04.2016].

UNITED STATES CENSUS BUREAU: U.S. and World Population Clock, en línea: http://www.census.gov/popclock/ [consultado el 4.04.2016].

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, en línea: https://www.congress.gov/bill/107th-congress/house-bill/3162 [consultado el 15.04.2016].

US-EU SAFE HARBOUR LIST, en línea: https://safeharbor.export.gov/list.aspx [25.04.2016].

LEGISLACIÓN

Recomendación de la OCDE sobre los principios relativos a la protección de la privacidad y transferencia internacional de datos personales, adoptada el 23 de septiembre de 1980.

Convenio nº 108 del Consejo de Europa, de 28 de enero, sobre protección de las personas en lo relativo al tratamiento automatizado de datos de carácter personal.

Reglamento (UE) 2016/679 del Parlamento 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.

Directiva 95/46/CE, del Parlamento 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.

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

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.

Ley Orgánica 1/1982, de 5 de mayo, de Protección Civil del Derecho al Honor, a la Intimidad Personal y Familiar y a la propia imagen

Tratado de Funcionamiento de la Unión Europea

Ley 9/1968, de 5 de abril, sobre secretos oficiales

ANEXO

1. **Cláusulas contractuales tipo:**

1.1. Decisión 2001/497/CE, de 15 de junio de 2001 relativa a cláusulas contractuales tipo para la transferencia de datos personales a un tercer país:

https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/decisiones/common/pdfs/Dec_2004_915_CE_271204_vers_consoli.pdf [consultado el 10.05.2016].

1.2. Decisión 2010/87/UE 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:

https://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/union_europea/decisiones/common/pdfs/decision_comm_clausulas_contractuales_2010.pdf [consultado el 10.05.2016].

1.3. Modelo de cláusulas contractuales AEPD para transferencias internacionales de datos entre encargado y subencargado del tratamiento:

https://www.agpd.es/portalwebAGPD/resoluciones/autorizacion_transf/common/pdfs/MODELO-DEFINITIVO-AEPD_Contrato-encargado-subencargado-21-03-2012.pdf [consultado el 10.05.2016].

2. **Reglas Corporativas Vinculantes o *Binding Corporate Rules:***

2.1. Preguntas más frecuentes sobre BCRs (WP 155):

https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/common/wp155_en.pdf [consultado el 10.05.2016].

2.2. Cuadro que establece la estructura de las BCRs (WP 154):

https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/common/wp154_en.pdf [consultado el 10.05.2016].

2.3. Cuadro que establece la relación de los elementos y principios que deben contener las BCRs (WP 153):

https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/common/wp153_en.pdf [consultado el 10.05.2016].

2.4. Modelo de solicitud de autorización de transferencia internacional basada en BCRs en el ámbito del procedimiento coordinado (WP 108):

https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/common/wp108_en.pdf [consultado el 10.05.2016].

2.5. Documento sobre la competencia de las Autoridades de Control europeas en el procedimiento coordinado de aprobación las BCRs (WP 107):

https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/common/wp107_en.pdf [consultado el 10.05.2016].

2.6. Documento sobre la aplicación del artículo 26.2 de la Directiva 95/46/CE a las BCRs (WP 74):

https://www.agpd.es/portalwebAGPD/canalresponsable/transferencias_internacionales/common/wp74_en.pdf [consultado el 10.05.2016].