Papeles de Derecho Europeo e Integración Regional

Working Papers on European Law and Regional Integration

MARÍA ÁLVAREZ CARO Y MIGUEL RECIO GAYO

Hacia un acuerdo Safe Harbour renovado para la transferencia internacional de datos entre EE.UU y la UE

WP IDEIR nº 25 (2015)

Cátedra Jean Monnet ● Prof. Ricardo Alonso García

Publicado por
Instituto de Derecho Europeo e Integración Regional (IDEIR)
Universidad Complutense
Facultad de Derecho
Avda. Complutense s/n
Madrid 28040 - España

ISSN 2172-8542

El presente proyecto ha sido financiado con el apoyo de la Comisión Europea. Esta publicación es responsabilidad exclusiva de su autor. La Comisión no es responsable del uso que pueda hacerse de la información aquí difundida.

Hacia un acuerdo Safe Harbour renovado para la transferencia internacional de datos entre EEUU y la UE

María Álvarez Caro[*] y Miguel Recio Gayo[**]

I. Antecedentes del acuerdo Safe Harbour: diferencias entre los sistemas de protección de datos personales entre la UE y EE.UU.— II. Decisión 2000/520/CE, Decisión de la Comisión Europea, de 26 de julio de 2000.— III. Principios generales.— IV. Especial atención a las autoridades de protección de datos. 1. Autoridades europeas de protección de datos. 2. La Comisión Federal de Comercio (FTC).— V. El Acuerdo en la era post-Snowden.— VI. Caso Schrems (C-362/14) y posibles implicaciones para el Puerto Seguro.— VII. Acuerdo de Puerto Seguro y computación en la nube. 1. El Puerto Seguro como un marco adecuado para la computación en la nube. 2. La Resolución de la AEPD en el expediente TI/00032/2014.— VIII. Experiencia en la aplicación de Safe Harbour y actualización del acuerdo.— IX. Algunas posibilidades para el futuro. 1. Reforzar el Acuerdo para restaurar la confianza y facilitar el comercio internacional. 2. Un nuevo acuerdo que sustituya al actual.

[*] María Álvarez Caro es Licenciada en Derecho por la Universidad de Oviedo; Máster en Protección de Datos, Transparencia y Acceso a la Información por la Universidad CEU San Pablo y Master en Business Administration (MBA) por el Instituto de Empresa (IE Business School). Es abogada colegiada del Ilustre Colegio de Abogados de Madrid. Actualmente trabaja en el Área Legal y de Relaciones Institucionales de la Asociación Española de la Economía Digital (adigital) y es profesora colaboradora del Master de Derecho de Propiedad Intelectual y Nuevas Tecnologías de la Universidad Autónoma de Madrid (UAM). Premio de investigación anual de la Cátedra Google de Privacidad, Sociedad e Innovación de la Universidad CEU San Pablo (I edición). Asimismo es autora de diversos artículos en revistas jurídicas y medios de comunicación.

[**] Miguel Recio Gayo es Licenciado en Derecho por la Facultad de Derecho de la Universidad Carlos III de Madrid; Máster en Protección de Datos, Transparencia y Acceso a la Información por la Universidad CEU San Pablo y Máster en Derecho de la Propiedad Intelectual por The George Washington University Law School (Estados Unidos). Es abogado en ejercicio del Ilustre Colegio de Abogados de Madrid. Actualmente trabaja como abogado y consultor en Derecho de las Tecnologías de la Información y las Comunicaciones (TIC). Anteriormente, trabajó como asesor legal para Latinoamérica para Business Software Alliance (BSA) en Washington, D.C. También trabajó en varias firmas jurídicas especializadas en Derecho de las TIC en Madrid. Premio de investigación anual de la Cátedra Google de Privacidad, Sociedad e Innovación de la Universidad CEU San Pablo (II edición). Es autor de diversas publicaciones en materia de protección de datos personales y otras áreas del Derecho de las TIC en España y en México.

I. ANTECEDENTES DEL ACUERDO SAFE HARBOUR: DIFERENCIAS ENTRE LOS SISTEMAS DE PROTECCIÓN DE DATOS PERSONALES ENTRE LA UE Y EE.UU.

El 25 de diciembre de 1998 entró en vigor la legislación general sobre protección de la vida privada en la Unión Europea, la Directiva 95/46/CE para la protección de datos personales[1]. En ella se dispone que sólo se podrán transferir datos personales a aquellos países no comunitarios[2] que ofrezcan un nivel adecuado de protección de la vida privada[3]. Si bien asimismo se contemplan una serie de excepciones en las que estaría permitida la transferencia de datos a un país que no garantiza un nivel adecuado de protección[4]. En este sentido, se trata de una lista exhaustiva de excepciones, a la que se añade una cláusula que permite la autorización de una transferencia internacional de datos personales por parte de Estados miembros a un tercer país que no garantice un nivel adecuado de protección para el supuesto de que el responsable del tratamiento ofrezca garantías suficientes con respecto a la protección de la vida privada, así como de los derechos y libertades fundamentales de las personas, que pueden derivarse de cláusulas contractuales adecuadas.

---

[1] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

[2] La referencia debe entenderse hecha al territorio de la Unión Europea, actualmente compuesta por 28 Estados Miembros, y los países del Espacio Económico Europea (Islandia, Liechtenstein y Noruega).

[3] El artículo 25 de la Directiva 95/46/CE dice así: "1. *Los Estados Miembros dispondrán que la transferencia a un país tercero de datos personales que sean objeto de tratamiento o destinados a ser objeto de tratamiento con posterioridad a su transferencia, únicamente puede efectuarse cuando, sin perjuicio del cumplimiento de las disposiciones de Derecho nacional adoptadas con arreglo a las demás disposiciones de la presente Directiva, el país tercero de que se trate garantice un nivel de protección adecuado. 2. El carácter adecuado del nivel de protección que ofrece un país tercero se evaluará atendiendo a todas las circunstancias que concurran en una transferencia o en una categoría de transferencias de datos; en particular, se tomará en consideración la naturaleza de los datos, la finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de Derecho generales o sectoriales, vigentes en el país tercero de que se trate, así como las normas profesionales y las medidas de seguridad en vigor en dichos países*. […]".

[4] En el artículo 26 de la Directiva 95/46/CE se recogen esas excepciones, que dice así: "1. *No obstante lo dispuesto en el artículo 25 y salvo disposición contraria del Derecho Nacional que regule los casos particulares, los Estados miembros dispondrán que pueda efectuarse una transferencia de datos personales a un país tercero que no garantice un nivel de protección adecuado con arreglo a lo establecido en el apartado 2 del artículo 25, siempre y cuando: a) el interesado haya dado su consentimiento inequívocamente a la transferencia prevista, o b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales tomadas a petición del interesado, o c) 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 o, d) la transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial, o e) la transferencia sea necesaria para la salvaguardia del interés vital del interesado o f) la transferencia tenga lugar desde un registro público que, en virtud de disposiciones legales o reglamentarias, esté concebido para facilitar información al público y esté abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan, en cada caso particular, las condiciones que establece la ley para la consulta. 2. […]"*

La aprobación de la Directiva 95/46/CE provocó cierta preocupación entre las empresas de Estados Unidos (EE.UU., en adelante), dado que la falta de una legislación sobre protección de datos comprehensiva en EE.UU. conducía a pensar que las empresas estadounidenses estarían limitadas en cuanto a su capacidad tanto para servir a los consumidores en la UE como para adquirir información sobre ellos[5]. Esta inquietud o preocupación llevó al Departamento de Comercio de EE.UU. a comenzar negociaciones con la Comisión Europa en 1998 para ver cómo se podían establece unos estándares de protección de datos satisfactorios[6], de modo que se permitiera ese flujo de datos necesario para numerosas empresas y, en general, para la economía americana.

Aunque (EE.UU) y la UE comparten el objetivo de mejorar la vida de sus ciudadanos, enfocan la protección de un modo diferente. La primera gran diferencia estriba en el hecho de que en la UE, la privacidad o el derecho a la protección de datos de carácter personal es un derecho fundamental reconocido como tal en las constituciones de los EE.UU, así como en la Carta de Derechos Fundamentales de la UE. Sin embargo, ni la Constitución Federal de EE.UU de 1787 ni ninguna de sus enmiendas, reconoce expresamente el derecho a la protección de datos personales o privacidad. Esta es la primera gran diferencia. Por otra parte, el planteamiento al otro lado del Atlántico es sectorial y tiene como fundamento una mezcla de legislación, reglamentación y autorregulación, mientras que en Europa, se trata de una legislación sumamente detallada y aplicable a todos los sectores[7]. En Europa impera un sistema *top-down*, frente a la descentralización en EE.UU. En el fondo, son diferencias que tienen su reflejo en el desarrollo digital de cada territorio y tienen un impacto en términos de innovación. "La economía digital en Europa ha sido lenta en acoger la revolución de los datos en comparación con EE.UU"[8].

"Para los americanos, la privacidad, aunque es un valor esencial, es vista como control sobre la información personal o lo que denominan *self determination* (autodeterminación informativa), mientras que en Europa se trata de un concepto más ligado a la dignidad y a un derecho humano o fundamental. Esta aproximación diferente en el punto de partida y en el enfoque de la materia de privacidad, también se traslada y es visible en el ámbito regulatorio"[9].

Dadas las diferencias, muchas entidades estadounidenses han expresado su inquietud sobre el nivel de adecuación que exige la UE para las transferencias de datos personales entre un territorio y otro. No obstante, a pesar de todas las diferencias entre ambos sistemas jurídicos –estas diferencias no sólo de sistemas jurídicos sino también diferencias

[5] Sunosky, James T: *Privacy online: A primer on the European Union's Directive and United State's Safe Harbour Privacy principles* en Soma, Jhon T.et al, "An analysis of the Use of Bilateral Agreements Between Transnational Trading Groups: The US /EU E-Commerce Privacy Safe Harbour", *Texas International Law Journal*, Vol. 39, 2008, pag.194.

[6] Algunos documentos relevantes sobre las negociaciones del Puerto Seguro, entre noviembre de 1998 y junio de 2000, pueden verse en la dirección de Internet http://export.gov/safeharbor/eu/eg_main_018496.asp

[77] Para ver las diferencias sobre el modo en el que se protege la privacidad en la UE en comparación con EE.UU, ver, entre otros, el documento de la Administración Obama, de mayo de 2014, *Big Data: Seizing opportunities, preserving value y Big Data and privacy: a technological perspective*.

[8] Comunicación de la Comisión Europea, de julio de 2014, *Towards a thriven data-driven economy*.

[9] Álvarez Caro, María e Uriarte Landa, Iñaki: "Dos visiones sobre la regulación de la privacidad y la innovación digital", Expansión (sección Jurídico), 12 de septiembre de 2014.

culturales- hay autores que defienden la aproximación que en los últimos años se ha producido en los sistemas de protección de la privacidad a ambos lados del Atlántico. Por ejemplo, el *reciente Consumer Privacy Bill of Rights*, de la Administración Obama, de 2012, es un ejemplo de esa aproximación de ambos sistemas. Aunque es cierto que en la UE, y en concreto en España donde tenemos una de las legislaciones más rigurosas en materia de protección de datos de carácter personal, disponemos de una legislación en materia de protección de datos muy proteccionista, es un error llegar a la conclusión de que en EE.UU la privacidad no se protege. De hecho, es un valor máximo, que ha tenido una protección y una construcción jurisprudencial[10].

En el momento en que dieron comienzo esas negociaciones entre la CE y el Departamento de Comercio de EE.UU, ambas partes tenían posturas bastante distanciadas. Por una parte, la FTC[11] (Federal Trade Commission) era más favorable a la autorregulación por la industria como el mejor método para otorgar protección de los datos personales con el menor impacto para el desarrollo económico[12]. Al contrario, la CE defendía firmemente la legislación comprehensiva y detallada en materia de protección de datos.

Entre 1998 y 1999, el Departamento de Comercio de EE.UU remitió a la CE varias propuestas o esquemas de autorregulación y todos ellos fueron rechazados por el Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE[13]. Durante los años 1998 y 1999 el GT29 emitió varios dictámenes o documentos sobre el nivel adecuado de protección de datos en las transferencias internacionales de datos, con especial atención a las negociaciones Safe Harbour entre EE.UU y la UE[14].

---

[10] Álvarez Caro, M.: *El derecho al olvido: el nuevo paradigma de la privacidad en la Era digital*, Colección de Derecho y Nuevas Tecnologías, Editorial Reus, Madrid, 2015, pag .XX.

[11] La FTC (Federal Trade Commision) es el organismo, que tiene naturaleza de agencia independiente, homólogo a nuestra Agencia Española de Protección de Datos (AEPD) que se encarga de velar por el respeto a la privacidad en las prácticas comerciales y publicitarias de las empresas. Este organismo, creado en 1914, trabaja para prevenir las prácticas engañosas, fraudulentas y desleales en el mercado, en protección del consumidor.

[12] Ver el documento de la FTC, *Self-Regulation and Privacy online: A report to Congress*, 1999.

[13] El Grupo de Trabajo del Artículo 29, creado por la Directiva 96/46/CE, es un órgano consultivo independiente integrado por las autoridades de protección de datos de los Estados miembros, el supervisor europeo de protección de datos y la Comisión Europea, que realiza funciones de secretariado. Este grupo de trabajo se encarga de estudiar toda cuestión relativa a la aplicación de las disposiciones nacionales tomadas para la aplicación de la Directiva, emitir dictámenes sobre el nivel de protección existente dentro de la UE y en países terceros, asesorar a la CE sobre cualquier proyecto de modificación de la Directiva y formular recomendaciones sobre cualquier asunto relacionado con la protección de datos de la UE. Puede verse más información sobre el mismo así como acceder a los documentos que publica, en http://ec.europa.eu/justice/data-protection/article-29/index_en.htm

[14] Ver los siguientes dictámenes o documentos del GT29 durante las negociaciones, en 1998 y 1999: Documento de Trabajo *Transfers of Personal Data to third countries: applying articles 25 and 26 of the EU Data Protection Directive*, 1998; *Opinion 1/99 concerning the level of Data Protection in the United States and the ongoing discussions between the European Commission and the United States Government*, 1999; *Opinion 2/1999 on the Adequacy of International Safe Harbour Principles ussued by the US Department of Commerce on 19th April 1999*.; *Working document on the current state of play of the ongoing discussions between the European Commission and the US Government concerning the International Safe Harbour Principles*, 07/09/1999.

II. DECISIÓN 2000/520/CE, DECISIÓN DE LA COMISIÓN EUROPEA, DE 26 DE JULIO DE 2000

La Decisión de la CE, 2000/520/CE, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de EE.UU, fue el resultado final de las negociaciones bilaterales durante dos años. Desde el establecimiento del acuerdo en el año 2000, más de 3.000 compañías americanas han suscrito el acuerdo de forma voluntaria. Las empresas que se adhieren a este acuerdo se comprometen a gestionar los datos personales conforme a los principios del acuerdo y disponen de una presunción de adecuación al nivel de protección exigido por la Directiva 95/46/CE.

En lo que respecta al ámbito de aplicación de la Decisión cabe destacar que no aplica ni a los sectores ni a los tratamientos de datos que no estén sujetos a la jurisdicción de los organismos estadounidenses enumerados en el Anexo VII de la citada Decisión[15]. Precisamente ésta, su ámbito de aplicación limitado, que se ciñe exclusivamente a aquellas materias o ámbitos sobre los que la FTC tiene jurisdicción[16], ha sido una de las críticas al sistema Safe Harbour. En la actualidad, el acuerdo está siendo objeto de revisión, conforme a lo establecido en el considerando 9 de la Decisión[17].

La Decisión en la que se plasma el acuerdo Safe Harbour consta de dos partes diferenciadas. Por un lado, los Principios y, por otro, las FAQ (*Frequently Asked Questions)*, en las que se proporciona orientación para aplicar los principios, publicadas por el Gobierno de EE.UU, el 21 de julio de 2000. Tal y como se señala en el artículo 1.2 de la Decisión: "*En relación con cada transferencia de datos deberán cumplir las siguientes condiciones: a) 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; b) 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*".

La decisión de adherirse a los requisitos de Puerto Seguro es totalmente voluntaria, tal y como consta en el Anexo I de la Decisión, en donde se recogen los principios de puerto seguro. El acuerdo Safe Harbour es la aplicación de los principios jurídicos de protección de datos de la UE por parte de entidades o empresas de EE.UU que voluntariamente se

[15] Dichos organismos son, por una parte, la FTC y, por otra parte, el Departamento de Transporte de Estados Unidos de América.

[16] Según se indica en el Anexo VII, ya citado, la FTC "*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 ganado"*.

[17] El Considerando 9 de la Decisión 2000/520/CE dice así: "*El puerto seguro creado por los principios y las FAQ puede precisar ser objeto de revisión teniendo en cuenta la experiencia adquirida, las novedades relativas a la protección de la vida privada en circunstancias que la tecnología hace cada vez más fácil la transferencia y tratamiento de datos personales, y los informes de aplicación elaborados por las autoridades correspondientes*".

adhieren a este sistema. La lista de entidades adheridas a los principios de Puerto Seguro está disponible en: http://www.export.gov/safeharbor/

III. PRINCIPIOS GENERALES

El Departamento Federal de Comercio de EE.UU publicó el 21 de julio de 2000 el documento con los Principios de Puerto Seguro, acompañado delas preguntas más frecuentes (FAQ) con orientaciones sobre cómo aplicar dichos principios. Estos últimos, se formularon en consulta con la industria y opinión pública, para facilitar el comercio y las transacciones entre EE.UU y la UE.

Tal y como se señala en el Anexo I, la adhesión a estos principios puede limitarse en los siguientes casos: "*a) cuando sea necesario para cumplir las exigencias de seguridad nacional, interés público y cumplimiento de la ley; b) por disposición legal o reglamentaria, o jurisprudencia que originen conflictos de obligaciones o autorizaciones explícitas, siempre que las entidades que recurran a tales autorizaciones puedan demostrar que el incumplimiento de los principios se limita a las medidas necesarias para garantizar los intereses legítimos esenciales contemplados por las mencionadas autorizaciones: c) por excepción o dispensa prevista en la Directiva o las normas de Derecho interno de los Estados miembros siempre que tal excepción o dispensa se aplique en contextos comparables. A fin de ser coherentes con el objetivo de mejorar la protección de la vida privada, las entidades deberán esforzarse en aplicar estos principios de manera completa y transparente, lo que incluye indicar en sus políticas de protección de la vida privada cuándo se aplicarán de manera regular las limitaciones a los principios permitidas por la anterior letra b). Por esta misma razón, cuando se permita la opción a tenor de los principios y/o de la legislación de EE.UU, se espera que las entidades opten por el mayor nivel de protección posible*".

El acuerdo recoge **siete principios**:

- **Notificación**: también conocido como deber de información. En base a este principio las entidades adheridas a este sistema de Safe Harbour deben informar a los interesados de las finalidades para las cuales han sido recabados sus datos así como de la identificación del responsable del fichero, con el fin de poder ejercitar los derechos ARCO (acceso, rectificación, cancelación u oposición). Es decir, son evidentes las semejanzas con lo dispuesto en nuestro artículo 5 de la Ley Orgánica de Protección de Datos (Ley Orgánica 15/1999, de 13 de diciembre).

- **Opción (choice):** Según, este principio, corresponde al interesado el poder decidir acerca de la finalidad y destino de sus datos de carácter personal, algo que se corresponde con nuestro principio del consentimiento del afectado o interesado, recogido en el artículo 6 de la LOPD.

- **Transferencia ulterior (transfer to third parties):** de acuerdo con este principio, sólo se permite la transferencia de datos cuando las entidades o países destinatarios estén suscritos al acuerdo Safe Harbour o sean Estados miembros de la UE, lo que viene a ser equivalente a lo dispuesto en el Título V de la LOPD.

- **Seguridad**: siguiendo con la equivalencia en la legislación española de protección de datos, este principio tiene su reflejo en el artículo 9 de la LOPD.

- **Integridad de los datos (data integrity):** hace referencia al principio de calidad.

- **Acceso:** como su propio nombre indica, encuentra su reflejo en el Titulo III de la LOPD, en los derechos ARCO.

- **Aplicación:** este principio hace referencia a la necesidad de articular mecanismos independientes de resolución de conflictos y de verificación del cumplimiento de los principios Safe Harbour, con potestad para sancionar, en su caso. En España, es la Agencia Española de Protección de Datos (en adelante, AEPD) quien tiene estas competencias.

Los principios básicamente reconocen los derechos de los titulares de los datos personales, imponen obligaciones a los responsables del tratamiento, establecen principios aplicables al procesamiento de la información y responsabilidad para el caso de infracción. Asimismo, las entidades deben adoptar mecanismos para garantizar la efectiva aplicación de los citados principios, tales como recursos independientes, procedimientos de monitoreo, medidas de reparación o sanciones[18].

IV. ESPECIAL ATENCIÓN A LAS AUTORIDADES DE PROTECCIÓN DE DATOS

Tal y como hemos señalado ya, la FTC, en virtud de las atribuciones que tiene conferidas, supervisa el cumplimiento del Acuerdo de Puerto Seguro por las organizaciones adheridas al mismo, de manera que es necesario prestar atención, a ambos lados del Atlántico, a cómo las autoridades de control son esenciales para impulsar también en la práctica el Puerto Seguro. Al mismo tiempo, es importante que como guardianas, en su caso, de la protección de datos o la privacidad, dichas autoridades colaboren con todas las partes interesadas para evitar obstáculos indebidos en las transferencias internacionales de datos al mismo tiempo que garantizan un alto nivel de protección de datos y privacidad con las medidas que les corresponden en virtud de las atribuciones y competencias que tienen asignadas.

Es por ello que, a continuación, se presta especial atención, respectivamente, a la posición que algunas autoridades europeas de protección de datos han adoptado en relación con el Acuerdo de Puerto Seguro así como algunas acciones de cumplimiento (en inglés, *"enforcement"*) de la FTC.

1. Autoridades europeas de protección de datos

Las autoridades europeas de protección de datos, tal como las ha calificado el Tribunal de Justicia de la Unión Europea, son las guardianas de los derechos fundamentales en lo que respecta al tratamiento de datos personales[19] y la FTC, en el caso EE.UU., es, desde

[18] Cerda, Alberto.: "El nivel adecuado de protección para las transferencias internacionales de datos personales desde la Unión Europea", *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, nº36, Universidad de Chile, agosto, 2011, pag.327 y ss.

[19] En este sentido, véase el apartado 23 de la sentencia del Tribunal de Justicia de la Unión Europea, de 9 de marzo de 2010, en el caso *Comisión/Alemania*, asunto C-518/07. En dicho apartado, el Tribunal de Justicia indica que *"las autoridades de control previstas en el artículo 28 de la Directiva 95/46 son las*

los años 70, la autoridad federal encargada de vigilar la política de privacidad y el cumplimiento de las normas en materia de privacidad sobre las que se le han conferido las potestades correspondientes en el caso de los Estados Unidos; sin perjuicio de que, en uno y otro caso, haya también autoridades reguladoras a considerar en ámbitos específicos o particulares. Salvando las distancias, debido a la diferente aproximación, respectivamente, en cuanto a la protección de datos y la privacidad, en ambos casos se trata de las autoridades encargadas de velar también por la protección de datos en el marco del Puerto Seguro.

Cabe señalar que, en la práctica, las autoridades europeas de protección de datos están desempeñando un papel diferente, ya que puede encontrarse desde posiciones que defienden en sus términos actuales el Acuerdo de Puerto Seguro, como ocurre en el caso de Irlanda, las que buscan la cooperación para asegurar el cumplimiento de la normativa sobre protección de datos personales y la privacidad, como por el ejemplo en el caso del Reino Unido, y otras que abogan por suspender el Acuerdo de Puerto Seguro.

En 2013, tras conocerse la existencia del programa PRISM a través de las revelaciones hechas por Edward Snowden, la Oficina del Comisionado de Protección de Datos de Irlanda (en inglés, *Office of the Data Protection Commissioner*), en respuesta a varias quejas recibidas no consideró necesario adoptar ninguna acción, como sí han hecho, por el contrario, las autoridades alemanas de protección de datos. Incluso la autoridad irlandesa firmó, con fecha 26 de junio de 2013, un memorándum de entendimiento (en inglés, *Memorandum of Understanding*, MoU) con la FTC[20]. Este memorándum, aunque no lo menciona expresamente, es también un instrumento importante para cooperar en el ámbito del Acuerdo de Puerto Seguro.

Por lo que se refiere al Reino Unido, la *Information Commissioner´s Office* (ICO) firmó, el 6 de marzo de 2014, un memorándum de entendimiento[21] con la FTC con la finalidad de reforzar la cooperación internacional. Se trata de un memorándum similar al que la autoridad irlandesa firmó también con la FTC.

Por el contrario, en el caso de Alemania, como veremos a continuación, sus autoridades de protección de datos, la federal y varias estatales, llevan anunciando desde hace varios

---

guardianas de los mencionados derechos y libertades fundamentales, y, como señala el considerando 62 de dicha Directiva, se estima que su creación en cada uno de los Estados miembros constituye un elemento esencial de la protección de las personas en lo que respecta al tratamiento de datos personales." La citada sentencia puede verse, en español, en la dirección de Internet http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d2dc30ddb7ea42fd5de447e4af04f5259cbcfc01.e34KaxiLc3qMb40Rch0SaxuQahj0?text=&docid=79752&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=528015

[20] El *"Memorandum of Understanding between the United States Federal Trade Commission and the Office of the Data Protection Commissioner of Ireland on mutual assistance in the enforcement of laws protecting personal information in the private sector"* está disponible en la dirección de Internet http://www.dataprotection.ie/documents/MOU/MOU.pdf

[21] El *"Memorandum of Understanding between the United States Federal Trade Commission and the Information Commissioner´s Office of the United Kingdom on mutual assistance in the enforcement of laws protecting personal information in the private sector"* está disponible en la dirección de Internet https://www.ftc.gov/system/files/attachments/international-competition-consumer-protection-cooperation-agreements/140306ftc-uk-mou.pdf Véase la nota de prensa, de 6 de marzo, al respecto en la dirección de Internet https://www.ftc.gov/news-events/press-releases/2014/03/ftc-signs-memorandum-understanding-uk-privacy-enforcement-agency

años, y ya casi de forma reiterada, procedimientos administrativos contra empresas estadounidenses adheridas al Puerto Seguro que darían lugar a suspender la aplicación del mismo por dudas sobre las garantías proporcionadas en cuanto a las transferencias de datos personales.

Se trata, por tanto, de situaciones que sirven para ilustrar cómo las autoridades de protección de datos pueden diferir significativamente en relación con un mismo asunto que tiene importantes implicaciones tanto para los titulares de los datos personales como las para las organizaciones que los tratan. Y, cualquier cambio en la aproximación o una aproximación diferente por las autoridades de protección de datos u otros actores involucrados puede tener también un importante impacto en la seguridad jurídica que se espera de un mecanismo como el Puerto Seguro.

1.1. Anuncios de acciones por las autoridades alemanas de protección de datos

A finales de enero de 2015, por citar en primer lugar la acción más reciente, en el marco de una conferencia[22] con motivo del día de la protección de datos[23], los Comisionados de Protección de Datos de Berlín y Hamburgo anunciaron el inicio de dos procedimientos administrativos, respectivamente en Berlín y Bremen, contra dos compañías estadounidenses que prestan servicios de nube en la Unión Europea y que podrían dar lugar a la suspensión de las transferencias en el marco del Acuerdo de Puerto Seguro.

Cabe señalar y es necesario tener en consideración que no es esta la primera vez en la que las autoridades alemanas de protección de datos anuncian la adopción de acciones en relación con el Puerto Seguro. Ya en 2010 un grupo de 16 autoridades con competencias sobre el sector privado, congregadas en un grupo de trabajo denominado *Düsseldorfer Kreis*, emitieron una resolución[24] en la que requerían a los exportadores de los datos que actuasen con una diligencia adicional al transferir datos personales en el marco del Acuerdo de Puerto Seguro[25].

Las autoridades alemanas, tanto federal como estatales, de protección de datos también se pronunciaron sobre el Puerto Seguro en julio de 2013 cuando emitieron una nota de prensa en la que manifestaron que, debido a las revelaciones sobre las actividades de vigilancia por los servicios de inteligencia y las agencias de seguridad, no emitirían nin-

[22] Al respecto, puede verse, por ejemplo, la nota de prensa de fecha 5 de febrero de 2015, en la dirección de Internet http://www.dataguidance.com/dataguidance_privacy_this_week.asp?id=3201

[23] Que se celebra cada 28 de enero desde el año 2007 en conmemoración de la fecha en la que se abrió a su firma el Convenio 108 del Consejo de Europa.

[24] Se trata de la *Decision by the supreme supervisory authorities for data protection in the nonpublic sector on 28/29 April 2010 in Hannover [revised version of 23 August 2010]*, que tiene por objeto específicamente la auto-certificación del importador de los datos. Puede verse, en inglés, en la dirección de Internet http://www.datenschutz-berlin.de/attachments/710/Resolution_DuesseldorfCircle_28_04_2010EN.pdf?1285316129

[25] Sobre esta resolución, puede verse también McBride, Naomi, Sotto, Lisa J. y Treacy, Bridget (2013), *Privacy & Data Security: The Future of the US-EU Safe Harbor*. Disponible, en inglés, en la dirección de Internet https://www.huntonprivacyblog.com/files/2013/12/Privacy-Data-Security-The-Future-of-the-US-EU-Safe-Harbor.pdf

guna aprobación más de transferencia internacional de datos y que considerarían suspender las transferencias internacionales de datos que se estaban llevando a cabo en virtud del Acuerdo de Puerto Seguro[26].

El anuncio de dichos procedimientos administrativos u otras acciones como las señaladas dan lugar a cuestionar, desde el punto de vista de las autoridades de protección de datos alemanas, la validez del Acuerdo de Puerto Seguro y, al mismo tiempo, la necesidad de que cualquier propuesta o acción que lleven a cabo las autoridades europeas de protección de datos sea coherente y, preferiblemente, consensuada cuando pueda tener repercusiones internacionales.

En concreto, es posible atender al hecho de que la autoridad federal alemana de protección de datos (en alemán, *Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit*) ha sido tajante y ha manifestado que el Acuerdo de Puerto Seguro no proporciona un nivel suficiente de protección de datos que permita la transferencia de datos en virtud del mismo[27].

Además, estos procedimientos administrativos habrían servido también, en su caso, como medida de presión en relación con las garantías que la Unión Europea quiere que se proporcionen, siendo buena muestra de ello las declaraciones de la Comisaria de Justicia, Consumidores e Igualdad de Género de la Unión Europea[28] en las que indicaba que, por una parte, está la cuestión relativa a las transferencias sucesivas por las entidades adheridas al Acuerdo de Puerto Seguro a subcontratistas y socios de negocio y, por otra parte, el acceso y uso de los datos personales por los servicios secretos estadounidenses con fines de seguridad.

Además, llama la atención el hecho de que la Comisaria indicase que la suspensión del Acuerdo de Puerto Seguro es el "plan B", ya que una suspensión del mismo tendría un impacto negativo en las relaciones entre Estados Unidos y la Unión Europea, al mismo tiempo que se convertiría en un obstáculo para muchas empresas que, por múltiples razones, necesitan que se facilite la posibilidad de realizar transferencias transatlánticas de datos personales.

Al respecto, no se debe olvidar ni obviar que las transferencias internacionales de datos personales entre la Unión Europea y los Estados Unidos son también clave para impulsar el comercio, especialmente los servicios digitales, con lo que ello supone para la competitividad y la innovación en el marco de la economía digital.

No obstante, además de considerar específicamente, es decir, por separado, las cuestiones relativas a la dimensión comercial del Acuerdo de Puerto Seguro y, en su caso, el acceso y uso posterior por terceros con fines de seguridad nacional, sería conveniente que las

---

[26] La nota de prensa, en inglés, está disponible en la dirección de Internet http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/ErgaenzendeDokumente/PMDSK_SafeHarbor_Eng.pdf?__blob=publicationFile

[27] A través de un comunicado de prensa publicado con fecha 19 de marzo de 2015 y disponible, en alemán, en la dirección de Internet http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/89DSK-SafeHarbor.html?cms_sortOrder=score+desc&cms_templateQueryString=safe+harbor

[28] Una entrevista a la Sra. Věra Jourová en la que hace referencia a las negociaciones con Estados Unidos puede verse en la dirección de Internet http://www.euractiv.com/sections/infosociety/vera-jourova-we-will-be-strict-us-safe-harbour-312856

autoridades europeas de protección de datos, así como otros actores relevantes, tales como la Comisión Europea, el Parlamento Europeo y el Consejo de la Unión Europea, dialogasen previamente para adoptar una aproximación común con la finalidad de prevenir o evitar situaciones que, en última instancia, tienen un impacto relevante para las empresas europeas tanto en términos de cumplimiento de la normativa sobre protección de datos personales y también para los titulares de dichos datos.

2. La Comisión Federal de Comercio (FTC)

Es necesario recordar aquí, una vez más, cuál es el papel de la FTC en relación con el Acuerdo de Puerto Seguro, ya que su gestión corresponde al Departamento de Comercio (en inglés, U.S. *Department of Commerce*), mientras que la FTC proporciona el respaldo necesario para su cumplimiento[29] donde tiene jurisdicción a tal fin.

2.1. Algunas acciones llevadas a cabo

Si bien durante los diez primeros años de funcionamiento del Acuerdo de Puerto Seguro no se recibieron quejas, por lo que no hubo ninguna acción sancionadora por parte de la FTC, desde 2009 sí se han llevado a cabo acciones por ésta contra organizaciones por declaraciones falsas en relación con el Puerto Seguro.

En concreto, tal como se indica en la Comunicación de la Comisión sobre el funcionamiento del Puerto Seguro[30], entre el 2009 y el 2012, se habían iniciado un total de diez (10) acciones[31], entre las que la Comisión destaca las de los casos Google, Facebook y MySpace.

---

[29] Tal como indicaba la Presidenta de la FTC, Edith Ramirez, en una carta de fecha 12 de noviembre de 2013, a la Vicepresidenta de la Comisión Europea sobre Justicia, Derechos Fundamentales y Ciudadanía, Viviane Reding, *"The U.S. Departament of Commerce administers the framework, and the FTC provides an enforcement backsstop."* (lo que puede traducirse al castellano como: *"El Departamento de Comercio de EE.UU. administra el marco y la FTC proporciona un apoyo para su cumplimiento."*) El título de la carta es *"Privacy Enforcement and Safe Harbor: Comments of FTC Staff to European Commission Review of the U.S.-E.U. Safe Harbor Framework"*. La carta, en inglés, puede verse en https://www.ftc.gov/sites/default/files/documents/public_statements/privacy-enforcement-safe-harbor-comments-ftc-staff-european-commission-review-u.s.eu-safe-harbor-framework/131112europeancommissionsafeharbor.pdf

[30] 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, COM(2013) 847 final, Bruselas, 27 de noviembre de 2013. Disponible en la dirección de Internet http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52013DC0847&rid=1

[31] Son las relativas a Javian Karnani, and Balls of Kryptonite, LLC (véase https://www.ftc.gov/enforcement/cases-proceedings/092-3081/best-priced-brands-llc-et-al), World Innovators, Inc. (véase https://www.ftc.gov/enforcement/cases-proceedings/0923137/world-innovators-inc-matter), ExpatEdge Partners, LLC (véase https://www.ftc.gov/enforcement/cases-proceedings/0923138/expatedge-partners-ll), Onyx Graphics, Inc. (véase https://www.ftc.gov/enforcement/cases-proceedings/0923139/onyx-graphics-inc), Directors Desk LLC (véase https://www.ftc.gov/enforcement/cases-proceedings/0923140/directors-desk-ll), Progressive Gaitways LLC (véase https://www.ftc.gov/enforcement/cases-proceedings/0923141/progressive-gaitways-ll), Collectify LLC (véase https://www.ftc.gov/enforcement/cases-proceedings/092-3142/collectify-ll), Google Inc. (véase https://www.ftc.gov/enforcement/cases-proceed-

En 2014 la FTC, en virtud de sus funciones y atribuciones, ha adoptado medidas de carácter administrativo contra diversas organizaciones que falsamente afirmaban estar en la lista de entidades adheridas al Puerto Seguro o, en su caso, mantener actualizada la autocertificación necesaria. En concreto, el 25 de junio de 2014, tras las investigaciones y acuerdos correspondientes, la FTC anunció[32] la aprobación de órdenes que establecían cargos (en inglés, *"final order settling charges"*)[33] contra un total de catorce (14) organizaciones, además de otras tres en el marco del Acuerdo de Puerto Seguro entre Estados Unidos y Suiza[34].

Y a las anteriores se suma otra medida más, también de carácter administrativo, que fue anunciada en abril de 2015 y que se refiere a una empresa que había dejado de estar adherida al Acuerdo de Puerto Seguro si bien mantenía una referencia a su participación en el mismo en su sitio web[35].

Es así que, por lo que se refiere al Acuerdo de Puerto Seguro entre la Unión Europea y los Estados Unidos, han sido veinticinco (25) las compañías sancionadas[36] (hasta mayo

---

ings/102-3136/google-inc-matter), Facebook, Inc. (véase https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc) y Myspace LLC (véase https://www.ftc.gov/enforcement/cases-proceedings/102-3058/myspace-llc-matter).

[32] Véase la nota de prensa, en la fecha mencionada, disponible en la dirección de Internet https://www.ftc.gov/news-events/press-releases/2014/06/ftc-approves-final-orders-settling-charges-us-eu-safe-harbor

[33] Sobre estas *"final orders"* así como sobre la autoridad de aplicación ("enforcement authority") de la FTC, puede verse *"A Brief Overview of the Federal Trade Commission´s Investigative and Law Enforcement Authority"*, disponible, en inglés, en la dirección de Internet https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority

[34] En cuanto al Acuerdo de Puerto Seguro entre Estados Unidos y Suiza puede verse más información, en inglés, en la dirección de Internet http://export.gov/safeharbor/swiss/index.asp

[35] Al respecto, puede verse la nota de prensa publicada por la FTC en https://www.ftc.gov/news-events/press-releases/2015/05/ftc-approves-final-orders-us-eu-safe-harbor-cases En cuanto al caso, se trata de la acción contra Tes Franchising, LLC (véase https://www.ftc.gov/enforcement/cases-proceedings/152-3015/tes-franchising-llc-matter).

[36] Se trata, además de las ya indicadas, de American Apparel, Inc. (véase https://www.ftc.gov/enforcement/cases-proceedings/142-3036/american-apparel-inc-matter); Apperian, Inc. (véase https://www.ftc.gov/enforcement/cases-proceedings/142-3017/apperian-inc-matter); Atlanta Falcons Football Club, LLC (https://www.ftc.gov/enforcement/cases-proceedings/142-3018/atlanta-falcons-football-club-llc-matter); Baker Tilly Virchow Krause, LLP (véase https://www.ftc.gov/enforcement/cases-proceedings/142-3019/baker-tilly-virchow-krause-llp-matter); BitTorrent, Inc. (véase https://www.ftc.gov/enforcement/cases-proceedings/142-3020/bittorrent-inc-matter); Charles River Laboratories International, Inc. (véase https://www.ftc.gov/enforcement/cases-proceedings/142-3022/charles-river-laboratories-intl-matter); DataMotion, Inc. (https://www.ftc.gov/enforcement/cases-proceedings/142-3023/datamotion-inc-corporation-matter); DDC Laboratories, Inc. (véase https://www.ftc.gov/enforcement/cases-proceedings/142-3024/ddc-laboratories-inc-also-dba-dna-diagnostics-center-matter); Fantage.com, Inc. (https://www.ftc.gov/enforcement/cases-proceedings/142-3026/fantagecom-inc-matter); Level 3 Communications, LLC (https://www.ftc.gov/enforcement/cases-proceedings/142-3028/level-3-communications-llc-matter); PDB Sports, Ltd., d/b/a[36] Denver Broncos Football Club (https://www.ftc.gov/enforcement/cases-proceedings/142-3025/pdb-sports-ltd-dba-denver-broncos-football-club-matter); Reynolds Consumer Products, Inc. (https://www.ftc.gov/enforcement/cases-proceedings/142-3030/reynolds-consumer-products-inc-matter); Receivable Management Services Corporation (https://www.ftc.gov/enforcement/cases-proceedings/142-3031/receivable-management-services-corporation-matter) y Tennesse Football, Inc. (https://www.ftc.gov/enforcement/cases-proceedings/142-3032/tennessee-football-inc-matter).

de 2015) por los motivos indicados anteriormente y se les ha ordenado que no *"tergiversen de cualquier manera, expresa o implícitamente, el alcance en el que demandado es miembro de, se adhiere a, cumple con, está certificado por, recibe la aprobación de, o de otra manera participa en cualquier programa de privacidad o seguridad patrocinado por el gobierno o cualquier otra organización de autorregulación o normalización, incluyendo, pero no limitado, al Marco de Puerto Seguro entre los EE.UU. y la UE"*[37].

No obstante, se trata de un número de acciones que debe considerarse a la vista del hecho de que en 2013 habría más de 400 incumplimientos, habiéndose duplicado el número en los últimos años[38], en concreto, desde 2008, cuando el número era de 200. Ahora bien, a su vez, estas cifras deben verse también a la luz de las críticas que señalan que no todos los incumplimientos suponen una infracción del Acuerdo de Puerto Seguro[39].

En cualquier caso, la supervisión y las acciones de cumplimiento efectivas son clave para hacer posible que el Acuerdo de Puerto Seguro sea una opción adecuada para las empresas y para las personas cuyos datos personales son tratados, y dichas funciones corresponden a las autoridades involucradas[40].

Resulta claro que, a pesar de que durante los primeros años no hubo acción alguna, lo importante ahora no es plantear excusas si hubo incumplimientos y a quién le correspondía identificarlos o conocer de los mismos, en su caso. Todos los esfuerzos se deben poner en pensar qué medidas concretas son necesarias para buscar y conseguir la protección efectiva de la persona cuyos datos personales son objeto de tratamiento. Al mismo tiempo,

---

[37] Traducción al castellano de *"misrepresent in any manner, expressly or by implication, the extent to which respondent is a member of, adheres to, complies with, is certified by, is endorsed by, or otherwise participates in any privacy or security program sponsored by the government or any other self-regulatory o standard-setting organization, including, but not limited to, the U.S.-EU Safe Harbor Framework"*. Véase, por ejemplo, la orden del caso American Apparel, Inc., disponible en https://www.ftc.gov/system/files/documents/cases/140625americanappareldo.pdf. Pág. 2.

[38] Véase Bendiek, Annegret (2013), *Test of Partnership, Transatlantic Cooperation in Cyber Security, Internet Governance, and Data Protection*, disponible, en inglés, en http://www.swp-berlin.org/fileadmin/contents/products/research_papers/2014_RP05_bdk.pdf# En dicho document se cita un una investigación realizada por una firma de consultoría, Galexia, que en 2008 detectó 200 incumplimientos y en 2013 un total de 427. La citada investigación es la de Chris Connolly, *The U.S. Safe Harbor – Fact or Fiction? (Syd-ney: Galexia, December 2008)*; Chris Connolly, *EU/U.S. Safe Harbor – Effectiveness of the Framework in Relation to National Security Surveillance*, October 7, 2013 (Paper for the Hearing in the LIBE Committee).

[39] Véase *Privacy & Data Security: The Future of the US-EU Safe Harbor*, ya citado. En dicho artículo se indica que *"Although the study intended to use this finding to discredit the Safe Harbor, the false assertion of these organizations did not, in fact, constitute a violation of the Safe Harbor though they may constitute a deceptive trade practice violation of Section 5 of the FTC Act."* Lo que puede traducirse al castellano como *"Aunque el estudio pretende usar este hallazgo para desacreditar el Puerto Seguro, la falsa afirmación de estas organizaciones no constituye, de hecho, una infracción del Puerto Seguro aunque pueda constituir una práctica comercial desleal que infringe la Sección 5 de la Ley de la FTC."*

[40] En este sentido, el Parlamento Europeo ha indicado que *"Critics have, however, have long maintained that the enforcement regime around the Safe Harbour agreement is much too weak to guarantee real-world compliance."* (lo que puede traducirse al castellano como: *"Los críticos, sin embargo, han mantenido desde hace mucho que el cumplimiento del régimen en relación con el acuerdo de Puerto Seguro es demasiado débil para garantizar el cumplimiento en el mundo real."* Véase European Parliamentary Research Service (2014), *Potential and Impact of Cloud Computing Services and Social Network Websites*, Science and Technology Options Assessment, disponible en http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/513546/IPOL-JOIN_ET(2014)513546_EN.pdf Pág. 78.

la posibilidad de recurrir a mecanismos de resolución extrajudicial de litigios es una oportunidad[41] que debe considerarse en términos que permita generar confianza para todas las partes implicadas, debiendo ser razonablemente accesible y, en cualquier caso, efectiva para los titulares de los datos personales.

V. EL ACUERDO EN LA ERA POST-SNOWDEN

Las revelaciones hechas por Snowden sobre la vigilancia de la Agencia de Seguridad Nacional (en inglés, *National Security Agency*, NSA) de los Estados Unidos[42] han tenido un virulento impacto, especialmente, en la industria tecnológica que, al mismo tiempo, ha permeado en el ámbito de las relaciones entre Estados y no sólo en el ámbito de las relaciones entre los Estados Unidos y la Unión Europea, sino también entre los propios Estados miembros de esta última.

Al margen de que la Comisión Europea demande más y el refuerzo de las garantías para los ciudadanos europeos con respecto al uso de sus datos personales con fines de vigilancia por las autoridades estadounidenses, es necesario, por una parte, partir de los procedimientos y garantías existentes en la actualidad[43], y, por otra, considerar que dichos procedimientos se aplican a empresas, quienes tienen la obligación de cumplir con la legislación que les es aplicable y que, por tanto, se trata de una cuestión que requiere de acciones de entendimiento entre países u organizaciones supranacionales, como en el caso de la Unión Europea.

Es decir, las revelaciones de Snowden, en el ámbito de la seguridad nacional, están teniendo repercusiones en otros ámbitos, como por ejemplo en el Acuerdo de Puerto Seguro cuyos fines son meramente comerciales. Esto hace que sea necesario deslindar claramente unos casos, los relativos a la seguridad nacional y otros intereses legítimos, y otros, relativos a relaciones comerciales.

En relación con lo anterior, desde el punto de vista de las relaciones de la Unión Europea con los Estados Unidos, se debe tener también en consideración que las negociaciones en materia de seguridad siguen su propio camino así como la experiencia acumulada, por ejemplo, en el ámbito de la transferencia de datos de pasajeros[44].

---

[41] Al respecto, véase el apartado relativo a la resolución extrajudicial de litigios en la Comunicación COM(2013) 847, ya citada. Págs. 15 a 17.

[42] Sobre la NSA puede verse más información en la dirección de Internet https://www.nsa.gov/

[43] Al respecto, puede verse el documento titulado *"Five Myths Regarding Privacy and Law Enforcement Access to Personal Information in the European Union and the United States"*, disponible en la dirección de Internet http://photos.state.gov/libraries/useu/231771/PDFs/Five%20Myths%20Regarding%20Privacy%20and%20Law%20Enforcement_October%209_2012_pdf.pdf

[44] Las Decisiones 2004/496/CE relativa a la celebración de un Acuerdo entre la Comunidad Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de los datos de los expedientes de los pasajeros por las compañías aéreas al Departamento de seguridad nacional, Oficina de aduanas y protección de fronteras, de los Estados Unidos; y 2004/535/CE relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de los Estados Unidos, fueron objeto de la sentencia del Tribunal de Justicia de 30 de mayo de 2006. La sentencia puede verse en la dirección de Internet http://curia.europa.eu/juris/document/document.jsf?text=&docid=57549&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=397713

Es decir, las revelaciones de Snowden ha dado lugar a una situación que requiere de un tratamiento específico y a un nivel que requiere de medidas que garanticen la seguridad jurídica tanto para los titulares de los datos personales como para las empresas que tratan datos personales para el desarrollo de su actividad. Por tanto, la incidencia que dichas relevaciones pueden tener en el Acuerdo de Puerto Seguro debe ser tratada buscando soluciones que tengan en consideración el uso de datos personales que son tratados con fines comerciales con una finalidad distinta, como es la salvaguardia de la seguridad nacional y, por tanto, considerando también los intereses específicos que se plantean.

Entran, por lo tanto, en juego, otros instrumentos tales como el Acuerdo de Asistencia Judicial entre la Unión Europea y los Estados Unidos de América (en inglés, *Mutual Legal Assistance Agreement*, MLAA)[45] que entró en vigor en 2010 y continúa vigente. Y es necesario no perder de vista que se trata de cuestiones entre gobiernos[46] y autoridades que, en su caso, pueden implicar obligaciones para las empresas, de manera que es necesario que las reglas y obligaciones sean claras, estén sujetas a un debido proceso con todas las garantías, y, de nuevo, garanticen la seguridad jurídica necesaria para todas las partes. En este sentido, hay que recordar también que, en paralelo al Puerto Seguro, los EE.UU. y la UE están también negociando, desde el 29 de marzo de 2011, el acuerdo marco sobre la protección de datos en el ámbito de la cooperación policial y judicial *("Data Protection Umbrella Agreement")*[47] que tiene por objeto la protección de datos personales en las transferencias internacionales de datos entre la UE y los EE.UU. para garantizar el cumplimiento de las normas (en inglés, *"law enforcement purposes")*[48].

VI. CASO *SCHREMS* (C-362/14) Y POSIBLES IMPLICACIONES PARA EL PUERTO SEGURO

El Acuerdo de Puerto Seguro es también el centro de atención de una petición de decisión prejudicial presentada por el Tribunal Supremo (High Court) irlandés, el 25 de julio de 2014, al Tribunal de Justicia de la Unión Europea, y que se plantea en el marco de un litigo entre el Sr. Schrems y la Autoridad irlandesa de Protección de Datos[49].

---

[45] Dicho acuerdo fue publicado en el Diario Oficial de la Unión Europea L 181, de 19 de julio de 2003. Sobre dicho acuerdo así como el acceso al mismo, puede verse http://ec.europa.eu/world/agreements/prepareCreateTreatiesWorkspace/treatiesGeneralData.do?redirect=true&treatyId=5441

[46] En este sentido, la Comisión Europea ha indicado que: *"Es importante señalar que, si bien la UE puede actuar en ámbitos de su competencia, en especial con objeto de garantizar la aplicación de su legislación, la seguridad nacional sigue siendo competencia exclusiva de cada Estado miembro."* Véase, Comunicación de la Comisión al Parlamento Europeo y al Consejo, Restablecer la confianza en los flujos de datos entre la UE y EE.UU., COM(2013) 846, Bruselas, 27.11.2013, disponible en la dirección de Internet http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52013DC0846&qid=1433438586675&from=ES

[47] Sobre esta cuestión puede verse, en inglés, la publicación de la Comisión Europea titulada *Fact Sheet EU-US Negotiations on Data Protection*, June 2014. Disponible en http://ec.europa.eu/justice/data-protection/files/factsheets/umbrella_factsheet_en.pdf

[48] Al respecto, también puede verse el comunicado de prensa de la Comisión Europea titulado *La Comisión Europea pide a EE.UU. que restablezca la confianza en los flujos de datos entre la UE y EE.UU.*, de 27 de noviembre de 2013. Disponible en http://europa.eu/rapid/press-release_IP-13-1166_es.htm

[49] La sentencia del Tribunal Supremo irlandés, de 18 de junio de 2014, puede verse, en inglés, en la dirección de Internet http://www.dataprotection.ie/docimages/documents/DOC180614.pdf

En concreto, se plantean al Tribunal de Justicia de la Unión Europea dos cuestiones prejudiciales, que son las siguientes:

"1) En el marco de la resolución de una reclamación presentada ante una autoridad independiente a la que la ley ha conferido las funciones de aplicar y ejecutar la legislación en materia de protección de datos, en la que se afirma que se están transmitiendo datos personales a un tercer país (en el caso de autos, los Estados Unidos de América) cuya legislación y práctica no prevén supuestamente una protección adecuada de la persona sobre la que versan los datos, ¿está vinculada dicha autoridad en términos absolutos por la declaración comunitaria en sentido contrario contenida en la Decisión de la Comisión de 26 de julio de 2000 (2000/520/CE), habida cuenta de los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea (2000/C 364/01), no obstante lo dispuesto en el artículo 25, apartado 6, de la Directiva 95/46/CE?

2) O bien, con carácter subsidiario, ¿puede y/o debe realizar el titular del cargo su propia investigación del asunto a la luz de la evolución de los hechos que ha tenido lugar desde que se publicó por vez primera la Decisión de la Comisión?"[50]

El caso *Schrems*, asunto C-362/14, plantea por tanto una importante cuestión sobre si una autoridad europea de protección de datos puede ignorar una decisión de la Comisión sobre el nivel de adecuación de un tercer país, en este caso el Acuerdo de Puerto Seguro con los Estados Unidos[51].

La vista pública del caso ante el Tribunal de Justicia tuvo lugar el 24 de marzo de 2015. De acuerdo al Sr. Schrems[52] y conforme al propio calendario publicado por el Tribunal de Justicia, el 24 de junio de 2015 era inicialmente la fecha en la que el abogado general presentaría sus conclusiones, pero fue retrasada sin indicación de la nueva fecha[53].

Aunque habrá que esperar hasta que el Tribunal de Justicia se pronuncie, hay que tener en consideración que el Sr. Schrems, como usuario de Facebook, contactó a la Agencia irlandesa de Protección de Datos tras las revelaciones hechas por Edward Snowden. Al respecto, no debe olvidarse ni perderse de vista que el Acuerdo de Puerto Seguro se produce en el ámbito comercial, con lo que ello supone para la economía digital, de manera que la atención sobre las cuestiones planteadas por el Sr. Schrems adquieren todo su sentido en el ámbito del tratamiento de datos personales con fines de seguridad y, por tanto,

[50] Estas cuestiones prejudiciales fueron publicadas en el Diario Oficial de la Unión Europea C 351, de 6 de octubre de 2014. Disponible en la dirección de Internet http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62014CN0362&from=ES

[51] Sobre las posibles implicaciones de este caso en el acuerdo de puerto seguro, véase Kuner, Christopher (2015), *Safe Harbor before the EU Court of Justice*. Disponible, en inglés, en la dirección de Internet http://cjicl.org.uk/2015/04/13/safe-harbor-before-the-eu-court-of-justice/ En dicho artículo, el autor indica que se trata de un caso que versa sobre la legalidad de las transferencias de datos a los Estados Unidos bajo el sistema establecido por el Acuerdo de Puerto Seguro y también que la cuestión relativa al acceso a los datos por servicios de inteligencia es una cuestión que tiene que resolverse mediante un acuerdo político entre la Unión Europea y los terceros países. Y adelanta, ya que el Tribunal de Justicia de la Unión Europea tendrá que pronunciarse al respecto, que no hay una solución perfecta a las cuestiones planteadas por el caso *Schrems*.

[52] En el sitio web http://europe-v-facebook.org/EN/en.html, en una noticia con fecha 25 de marzo de 2015, se indica que *"The advocate general (Mr. Bot) will deliver his opinion on 24.6.2015."*

[53] El propio Sr. Schrems, en su sitio web ya citado, indicó, con fecha 9 de junio de 2015, que había sido informado de que se posponía la fecha inicialmente prevista, sin fijar una nueva fecha. Desaparecía también la referencia al mismo en el calendario del Tribunal de Justicia de la Unión Europea.

en lo que se refiere a actividades de seguridad nacional. En concreto, una de las cuestiones planteadas por la Comisión Europea para reestablecer la confianza en las transferencias de datos entre la Unión Europea y los Estados Unidos es que por parte de este último se mejore la supervisión de los programas de obtención de datos con fines de inteligencia mediante el fortalecimiento del papel del Tribunal de Vigilancia de Inteligencia Extranjera e introduciendo medios de recurso para las personas físicas, titulares de los datos[54].

Y lo anterior debe considerarse en relación con la recomendación propuesta por la Comisión de que las políticas de privacidad de auto-certificación de las compañías adheridas al Puerto Seguro incluyan información sobre el alcance relativo al acceso por autoridades públicas de obtener y tratar datos trasferidos en el marco del Acuerdo de Puerto Seguro. Así mismo, la Comisión recomienda que la excepción de seguridad nacional prevista en el Acuerdo de Puerto Seguro sea aplicada de manera estricta o proporcional[55].

Por último, la sentencia del Tribunal de Justicia de la Unión Europea podría aclarar cuál es el alcance de las decisiones de la Comisión Europea relativas a casos en los que se reconoce el nivel adecuado de un tercer país en sentido estricto. Es decir, aunque no se trate de un tercer país, ¿pueden las autoridades europeas de protección de datos pedir garantías adicionales a la propia Decisión de la Comisión Europea por la que se reconoce el nivel adecuado de las empresas adheridas al Acuerdo de Puerto Seguro?

VII. ACUERDO DE PUERTO SEGURO Y COMPUTACIÓN EN LA NUBE

1. El Puerto Seguro como un marco adecuado para la computación en la nube

Como marco que facilita las transferencias internacionales de datos hacia empresas establecidas en Estados Unidos, con lo que ello supone para el comercio internacional y en particular los servicios digitales, el Puerto Seguro es también un instrumento a tener en consideración por lo que se refiere a los servicios de computación en la nube (en inglés, *"cloud computing"*).

---

[54] En su memo, de 27 de noviembre de 2013, titulado *"Restoring Trust in EU-US data flows – Frequently Asked Questions"*, la Comisión, en respuesta a la pregunta *"How will the U.S. review of U.S. surveillance programmes benefit EU citizens?"* indica que *"The oversight of U.S. intelligence collection programmes would be improved by strengthening the role of the Foreign Intelligence Surveillance Court and by introducing remedies for individuals. These mechanisms could reduce the processing of personal data of Europeans that are not relevant for national security purposes."* Disponible en http://europa.eu/rapid/press-release_MEMO-13-1059_en.pdf

[55] En su memo, ya citado, la Comisión indica lo siguiente:

"Access by US authorities

1. Privacy policies of self-certified companies should include information on the extent to which US law allows public authorities to collect and process data transferred under the Safe Harbour. In particular companies should be encouraged to indicate in their privacy policies when they apply exceptions to the Principles to meet national security, public interest or law enforcement requirements.

2. It is important that the national security exception foreseen by the Safe Harbour Decision is used only to an extent that is strictly necessary or proportionate."

En concreto, una de las trece (13) recomendaciones que ha hecho la Comisión Europea para mejorar el Puerto Seguro es la relativa a que las empresas adheridas al mismo sean transparentes en cuanto a las condiciones de privacidad en los contratos que firmen con subcontratistas, como por ejemplo ocurre en el ámbito de los servicios de nube[56].

Las ventajas que implica la nube para las empresas, de cualquier tamaño, e incluso para los particulares, no deberían resultar afectadas por incertidumbres que pudieran plantearse en relación con el Acuerdo de Puerto Seguro ni por otras acciones que pudieran tener una incidencia negativa en las transferencias internacionales de datos.

En este sentido, en la práctica, la adhesión por un prestador de servicios de nube al Acuerdo de Puerto Seguro debería ser suficiente, desde el punto de vista de las autoridades europeas de protección de datos, para poder transferir datos personales por una organización establecida en la Unión Europea. Lo contrario supondría, por una parte, dejar sin efecto o, al menos, minusvalorar, medidas como el Acuerdo actual y, por otra parte, crear situaciones que podrían llegar a ser consideradas, en su caso, incluso como barreras al comercio.

En relación con lo anterior, específicamente por lo que se refiere a la computación en la nube, cabe prestar atención al Dictamen 5/2012 sobre la computación en la nube[57], adoptado por el Grupo de Trabajo del artículo 29 el 1 de julio de 2012. En dicho Dictamen el Grupo de Trabajo parte de que *"la autocertificación con puerto seguro por sí sola no puede considerarse suficiente en ausencia de una sólida aplicación de los principios de protección de datos en la computación en nube"*[58] y en relación con esto indica que *"las cláusulas tipo de conformidad con la Decisión 2010/87/CE de la Comisión son un instrumento que puede ser utilizado entre el encargado y el responsable del tratamiento como base para que la computación en nube ofrezca garantías adecuadas en el contexto de las transferencias internacionales."*[59]

En definitiva, que medidas como el Acuerdo de Puerto Seguro puedan ser ventajosas para las organizaciones, sin que ello suponga en modo alguno disminuir o renunciar a las garantías necesarias en materia de protección de datos, requiere que se busquen formas de promoverlas, lo que lleva a considerar que someter las transferencias internacionales en el marco del Acuerdo de Puerto Seguro a un procedimiento de autorización previa sobre la base de un clausulado contractual a adicional a que el importador de los datos personales esté adherido a aquél puede ser una especie de doble candado y, en la práctica, un desincentivo para que las empresas estadounidenses se adhieran al mismo. Es decir, con los ajustes necesarios, especialmente por lo que se refiere al acceso a los datos personales por terceros (solicitudes gubernamentales), y otros aspectos relevantes que deben ser monitorizados constantemente, el Acuerdo de Puerto Seguro es un mecanismo adecuado para facilitar la contratación y uso de servicios digitales, así como impulsar la competitividad, las inversiones y la innovación.

[56] Véase el memo de fecha 27 de noviembre de 2013, ya citado.

[57] Disponible en la dirección de Internet http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_es.pdf

[58] Pág. 20 del Dictamen.

[59] Pág. 21 del Dictamen.

2. La Resolución de la AEPD en el expediente TI/00032/2014

Un ejemplo de que en la práctica el Acuerdo de Puerto Seguro puede ser una solución relegada como consecuencia del Dictamen del Grupo de Trabajo del artículo 29 ya mencionado puede ser, en buena medida, la resolución de la Agencia Española de Protección de Datos (AEPD) en el expediente número TI/00032/2014, de fecha 9 de mayo de 2014, que tiene por objeto la declaración de adecuación de garantías para las transferencias internacionales de datos a los Estados Unidos con motivo de la prestación de servicios de computación en nube[60].

Sin perjuicio de las cuestiones específicas que se tratan en dicha resolución, la misma es, o puede ser, relevante a efectos del Acuerdo de Puerto Seguro por varios motivos.

En primer lugar, porque siendo el importador de los datos personales[61] una empresa adherida a dicho acuerdo[62], no se hace referencia al mismo. La razón de la falta de esta referencia en este caso puede deberse, aunque no lo diga la resolución, a que se trata de que el prestador de servicios de nube busca esta solución en virtud de lo previsto en el Dictamen 5/2012, al que ya nos hemos referido, y a la que se refiere la propia resolución. Es decir, además de estar adherido al Puerto Seguro, el prestador de nube tiene que buscar garantías adicionales.

Además, aunque sea una cuestión meramente incidental, cabe considerar que en España, hemos pasado de las previsiones de la Instrucción 1/2000 relativa a las normas por las que se rigen los movimientos internacionales de datos[63], que consideraba como un supuesto específico el caso del Acuerdo de Puerto Seguro[64], a otra situación totalmente

---

[60] La resolución puede verse en la dirección de Internet http://www.agpd.es/portalwebAGPD/resoluciones/autorizacion_transf/auto_transf_2014/common/pdfs/TI-00032-2014_Resolucion-de-fecha-09-05-2014_de-MICROSOFT-CORPORATION_a-Estados-Unidos.pdf

[61] Figura a la que se define en el Reglamento de la LOPD 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"* (art. 5.1.ñ).

[62] Lo que puede comprobarse a través de la dirección de Internet https://safeharbor.export.gov/list.aspx

[63] Se trata de la Instrucción 1/2000, de 1 de diciembre, de la Agencia Española de Protección de Datos, relativa a las normas por las que se rigen los movimientos internacionales de datos, publicada en el Boletín Oficial del Estado núm. 301, de 16 de diciembre de 2000 (la versión consolidada puede verse en http://www.boe.es/buscar/pdf/2000/BOE-A-2000-22726-consolidado.pdf). Dicha Instrucción fue derogada en virtud de la disposición derogatoria única del Real Decreto 1720/2007, de 21 de diciembre ("Reglamento de la LOPD").

[64] En concreto, la Norma cuarta de la Instrucción 1/2000, relativa a las "transferencias al territorio de Estados que otorguen un nivel adecuado", indicaba, en relación con la Decisión del acuerdo de puerto seguro, lo siguiente:

"3. Si la transferencia se funda en lo establecido en la Decisión 2000/520/CE de la Comisión de las Comunidades Europeas, «sobre la adecuación de la protección conferida por los principios de Puerto Seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de los Estados Unidos», quien pretenda efectuar la transferencia deberá acreditar que el destinatario se encuentra entre las entidades que se han adherido a los principios, así como que el mismo se encuentra sujeto a la jurisdicción de uno de los organismos públicos estadounidenses que figuran en el Anexo VII de la citada Decisión.

4. Lo indicado en el apartado anterior será de aplicación a todos los supuestos en que el nivel de protección adecuado se declare por la Comisión de las Comunidades Europeas en relación con un sistema de autorregulación o de condiciones similares a las contenidas en la Decisión 2000/520/CE."

distinta en el Reglamento de la LOPD[65] que lo incluye, sin más, entre los supuestos de terceros países sin nivel adecuado de manera que desaparece dicha referencia específica.

Es decir, en vez de tratarlo como cualquier otro supuesto de autorización para la transferencia internacional de datos a un país sin nivel adecuado, se podría haber mantenido, al menos, una mención específica a la Decisión de la Comisión Europea que, en la práctica, permitiese hacer posible que el nivel adecuado previsto en la misma pueda servir como base para obtener una autorización "automática" cuando el destinatario de dicha transferencia, el importador, sea una organización adherida a dicho acuerdo por concurrir las garantías suficientes necesarias.

El Dictamen del Grupo de Trabajo del artículo 29, una aproximación diferente por las autoridades europeas de protección de datos al Acuerdo de Puerto Seguro y una sentencia todavía pendiente del Tribunal de Justicia de la Unión Europea son también aspectos a considerar para, en su caso, poder evitar, en la medida de lo posible, situaciones complejas en el futuro, especialmente para las empresas que transfieren datos personales en el marco del Acuerdo de Puerto Seguro así como para los titulares de dichos datos.

Y en segundo lugar, porque tanto para el importador de los datos personales como para el exportador, sería positivo poder hacer uso de soluciones como un acuerdo que deben aplicar homogéneamente todas las autoridades europeas de protección de datos. Es decir, el Acuerdo de Puerto Seguro es también una medida que refuerza la seguridad jurídica, en términos de previsibilidad, tanto para el exportador de datos personales[66] como para el importador de los mismos. Y no es sólo una cuestión de política pública, favorecer las transferencias de datos personales en un marco que asegure las garantías necesarias, sino además una necesidad para un entorno de servicios digitales que requieren de soluciones adecuadas ante una economía global digital.

En particular, cabe señalar que la resolución parte de proporcionar una autorización para la transferencia internacional de datos, que puede considerase como especial, ya que es solicitada por el importador y no por el exportador[67], pero lo hace a la luz del esquema general previsto en los artículo 33 de la LOPD y 70 de su Reglamento de desarrollo, relativos a la norma general de prohibición de transferencias a terceros países sin nivel adecuado sin hacer mención o referencia alguna a la Decisión de la Comisión Europea sobre el Acuerdo de Puerto Seguro.

Sin perjuicio de lo anterior y al margen del caso específico, esta resolución sirve para poner de manifiesto que el Reglamento de la LOPD, en su artículo 70, relega al Acuerdo

---

[65] 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 ("Reglamento de la LOPD"). La versión consolidada puede verse en http://www.boe.es/buscar/pdf/2008/BOE-A-2008-979-consolidado.pdf

[66] Al que se define en el Reglamento de la LOPD como *"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"* (art. 5.1.j).

[67] Véase, en este sentido, que la resolución indica que "El supuesto objeto de análisis en la presente resolución reviste ciertas especialidades respecto de los que han venido tradicionalmente siendo objeto de resoluciones de autorización de transferencias internacionales de datos. Ello se debe, en primer lugar, al hecho de que la documentación que ha de ser analizada ha sido presentada no por el exportador, sino por el importador de datos personales." (Fundamento de Derecho III, pág. 3).

de Puerto Seguro a ser un instrumento casi virtual ya que como hemos señalado, a diferencia de la Instrucción 1/2000, el Reglamento omite cualquier referencia al mismo como garantía adecuada para las transferencias internacionales de datos a las organizaciones adheridas al Puerto Seguro. Habrá que ver, por tanto, si el caso *Schrems* permite tener más claridad al respecto.

En definitiva, ya sea a nivel nacional o europeo, es necesario que el Acuerdo de Puerto Seguro se convierta también en una medida que sirva como instrumento para impulsar la prestación de servicios de nube y cualesquiera otros, ya que, especialmente, las PYMEs pueden beneficiarse de servicios digitales que les permitan ser más eficientes y competitivas, ya sea en mercados locales o incluso en un mercado global.

VIII. EXPERIENCIA EN LA APLICACIÓN DE SAFE HARBOUR Y ACTUALIZACIÓN DEL ACUERDO

Después de la preocupación por las noticias relativas a los programas de vigilancia de EE.UU, la ex comisaria de Justicia de la UE, Viviane Reding, anunció en julio de 2013 que la Comisión pretendía realizar un análisis (assessment) del acuerdo Safe Harbour. Desde que se ha venido aplicando Safe Harbour no ha estado exento de críticas. Como ya hemos mencionado, en julio de 2012, el GT29, en su Dictamen (Opinion) sobre Cloud Computing[68], sugería que los exportadores de datos de la UE no podían apoyarse sólo en la autocertificación de adhesión a Safe Harbour por parte del proveedor de servicios de cloud para legitimar las transferencias de datos personales. Al contrario, en abril de 2013, el Departamento de Comercio de EE.UU reconocía Safe Harbour como un mecanismo legítimo para la transferencia de datos en el ámbito del Cloud.

En abril de 2004, la Comisión Europa elaboró un detallado estudio sobre el estado de aplicación de Safe Harbour[69] en EE.UU. Este análisis ponía de manifiesto deficiencias notorias, entre las que cabe destacar:

- Falta de transparencia o información defectuosa, falta de claridad de las políticas de privacidad y de las finalidades o actividades para las cuáles se llevaban a cabo tratamientos de datos, lo que hacía que, en la práctica, el principio de notificación o deber de información quedase, en ocasiones, en papel mojado.

- En relación con las transferencias a terceros, se detectó, en ocasiones, una falta de definición con respecto al concepto de tercero y, en algunos casos, no había un compromiso de ese tercero (socio, filial, empresa de un grupo de empresas, etc…) de cumplir con los principios de Safe Harbour. La CE destacó que la flexibilidad con la que había sido configurado el principio de "transferencia ulterior" o "transfer to third parties", lo convertía en una vía efectiva para eludir la legislación de la UE.

- En relación con el Acceso, la información que se ofrecía al respecto por parte de las empresas era muy vaga e imprecisa, hasta el punto de que se ofrecía una dirección de

[68] Ver la Opinion del GT29 sobre Cloud Computing de 1 de julio de 2012.

[69] Ver el documento de trabajo de los servicios de la Comisión: *The implementation of Commission Decission 520/2000/CE on the adequate protection of personal data provided by the safe harbour privacy principles and related FAQs issued by the US Department of Commerce*, SEC (2004), 1323, de 20 de octubre de 2004.

contacto en el mejor de los casos, pero no se explicaban con detalle los derechos que el titular de los datos podía ejercitar.

- La información sobre las actividades y finalidades era escasa, lo que repercutía también en el incumplimiento, en ocasiones, del principio de calidad, al ser difícil valorar la pertinencia de los datos de conformidad con los fines para los que son recabados.

Por otra parte, más allá de este estudio de la CE de 2004, en relación con la aplicación práctica de Safe Harbour, han evidenciado otras deficiencias como el descontrol en lo que respecta de las empresas adheridas a este marco, como listados desfasados de empresas.

En noviembre de 2013, la CE publicó la Comunicación al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE. Aquí, la CE destacó que "*existe una inquietud creciente entre algunas autoridades de protección de datos de la UE respecto a las transferencias de datos en el actual marco de puerto seguro. Las autoridades de protección de datos de algunos Estados miembros critican la formulación excesivamente general de los principios, así como la fuerte dependencia de la autocertificación y la autorregulación. La industria ha expresado preocupaciones similares referentes a distorsiones de la competencia debidas a la falta de aplicación*"[70].

En la actualidad, EE.UU y la UE están negociando de cara a la actualización del acuerdo Safe Harbour. Las transferencias de datos resultan vitales para el desarrollo de las empresas y, por ello, el logro del éxito en estas negociaciones es fundamental. De otro modo, se impondrían obstáculos al normal desenvolvimiento de las empresas y supondría dar marcha atrás o rechazar un acuerdo que, aunque con sus más y sus menos y con aspectos mejorables, es un marco eficaz, que proporciona seguridad jurídica y ha venido funcionando durante años.

En relación con lo que supone el Acuerdo Seguro para la economía digital, la Subsecretaria para el Crecimiento Económico, Energía y Medioambiente de los Estados Unidos[71], en una visita a Bruselas a principios de junio de 2015, se refirió específicamente a esta cuestión manifestando que éste es un claro ejemplo del puente que es necesario entre ambas potencias económicas, especialmente para las PYMEs, ya que más del 60% de empresas adheridas al mismo lo son[72].

---

[70] Ver la página 5 de la citada Comunicación de la CE, de 27 de noviembre de 2013.

[71] La Sra. Catherine A. Novelli, quien tiene el cargo de Under Secretary for Economic Growth, Energy, and the Environment.

[72] En concreto, la Subscretaria indicó que *"At the same time, vast new data flows raise a number of privacy and security issues that need to be addressed to maintain the confidence of businesses, researchers, innovators, and ordinary citizens in the system. The United States and Europe need to bridge any differences in a way that will keep our transatlantic digital economy healthy. The Safe Harbor Framework is a strong example of one such bridge.*

Since it was established 15 years ago, almost 3500 organizations across a broad range of industries have become Safe Harbor certified. These include large, multination corporations, medium sized firms, but also a surprisingly large number of small and medium enterprises, more than 60 percent of Safe Harbor companies are SMEs. By strengthening and affirming the Safe Harbor framework, we can effectively work with European partners to ensure that data can be transferred across borders freely and securely. We look forward to concluding the renegotiations in the very near future." La nota de prensa con los comentarios, publicada por el Departamento de Estado de los Estados Unidos, puede verse, en inglés, en http://www.state.gov/e/rls/rmk/243086.htm

IX. ALGUNAS POSIBILIDADES PARA EL FUTURO

Renovar el Acuerdo de Puerto Seguro es el objetivo, ya sea a través de reforzar algunos aspectos de la versión actual o, incluso, mediante un nuevo acuerdo. En cualquier caso, hay que buscar soluciones duraderas que permitan desarrollar en un marco de confianza la economía digital, con las máximas garantías para el derecho fundamental a la protección de datos o la privacidad, teniendo en consideración la experiencia acumulada.

1. Reforzar el Acuerdo para restaurar la confianza y facilitar el comercio internacional

Entre las varias opciones que pueden darse en torno al Acuerdo de Puerto Seguro actual, una es la de reforzarlo con base en la experiencia acumulada durante los últimos años y el hecho de que los actores involucrados a ambos lados del Atlántico han tratado ya diversos aspectos y diferentes cuestiones en relación con el mismo.

Reforzar el Acuerdo de Puerto Seguro, además de que sea una necesidad, es una medida positiva que debe servir para impulsar el comercio internacional y la prestación de servicios digitales, sin perder de vista que es una oportunidad para las empresas, especialmente las europeas. No poder hacer uso de mecanismos como el Acuerdo de Puerto Seguro tendría consecuencias negativas tanto para las empresas como para los titulares de los datos personales[73].

Es también importante tener en consideración que las recomendaciones[74], partiendo de que sean viables, requieren de seguimiento, que debe ser ágil si se quiere garantizar la efectividad y continuidad de una solución como el Acuerdo de Puerto Seguro. Dilatar o posponer la toma de ciertas decisiones, con independencia de las repercusiones comerciales que pueden tener las mismas y más allá de éstas, es una cuestión que tiene incidencia tanto para el comercio internacional, como para la competitividad de las empresas, la innovación y la garantía de los derechos de las personas, ya sea la privacidad de los consumidores o el derecho fundamental de los titulares de los datos, que en cualquier caso coinciden en la garantía de control sobre el tratamiento de sus datos personales. Y lo anterior es clave para generar o, en su caso, reforzar también la confianza de todas las partes implicadas.

Es así que el Acuerdo de Puerto Seguro constituye una oportunidad, aunque no única ya que existen o pueden darse otras soluciones, que debe impulsarse a través de reglas claras, adecuadas para los fines que se buscan en cuanto promover el comercio digital internacional, y que sin duda requiere de garantías que se concreten en un nivel de cumplimiento efectivo en caso de que se cometan infracciones. Y dicho nivel de cumplimiento no es sólo una cuestión que recaiga en la FTC u otras autoridades reguladoras que puedan tener

[73] La Comisión Europea indica, en su COM(2013) 846 final, ya citada, que: *"su derogación afectaría negativamente a los intereses de las empresas de la UE y de los Estados Unidos que se han adherido al mismo"* (pág. 8).

[74] De nuevo, deben considerarse las recomendaciones hechas por la Comisión Europea, tal y como se indica en el memo de fecha 27 de noviembre de 2013, ya citado.

competencias al respecto, sino que requiere de la participación de las autoridades europeas de protección de datos.

Ahora bien, reforzar el Acuerdo de Puerto Seguro no es la única opción que puede plantearse, pero sí que debe considerarse a la hora de avanzar en la consecución de objetivos en vista de lo ya conseguido hasta el momento.

2. Un nuevo acuerdo que sustituya al actual

Otra opción posible es la de un nuevo acuerdo que sustituya al actual. Tras quince años de experiencia acumulada y teniendo en consideración todo lo que ha sucedido, e incluso está por suceder, como pueden ser las revelaciones de Snowden hace tan sólo unos años o la sentencia del Tribunal de Justicia de la Unión Europea en el caso *Schrems* (esperada para el otoño de 2015), un nuevo acuerdo podría significar dejar atrás el pasado, evitando tener que enmendar un texto con el que quizás algunos se sentirían incómodos y tener la oportunidad de avanzar firmemente sobre un instrumento nuevo.

Son innumerables los documentos que tanto la FTC como la Comisión Europea o el Parlamento Europeo, entre otros actores, han publicado durante los últimos años en relación con el Acuerdo de Puerto Seguro. Desde informes de evaluación[75] hasta las más recientes Comunicaciones de la Comisión Europea[76]. Y son también numerosas las notas de prensa que, a uno y otro lado del Atlántico, se han dedicado al mismo.

Incluso no han sido pocas las ocasiones en las que bien se ha anunciado que el Puerto Seguro podría quedar suspendido[77] o bien, por el contrario, el deseo de finalizar las negociaciones sobre la revisión del acuerdo, siendo una de las más relevantes la hecha a través de la Declaración de Riga, el 3 de junio de 2015, con motivo del Encuentro de Justicia y Asuntos de Interior de la UE y de los EE.UU.[78] No obstante, una vez más, los plazos que se habían dado las partes siguen posponiéndose como si se tratara de un bucle

[75] Véase una primera revision en 2002 en el documento Commission Staff Working Paper, The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce, SEC(2002) 196, Bruselas, 13.2.2002, disponible, en inglés, en http://ec.europa.eu/justice/policies/privacy/docs/adequacy/sec-2002-196/sec-2002-196_en.pdf También, puede verse una segunda revisión, publicada a través del documento Commission Staff Working Document, The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce, disponible, en inglés, en http://ec.europa.eu/justice/policies/privacy/docs/adequacy/sec-2004-1323_en.pdf

[76] Se trata, por una parte, de la ya citada COM(846) 2013,, y, por otra parte, de la COM(2013) 847 final, ya citada.

[77] Por ejemplo, la Sra. Viviane Reding, por entonces Vicepresidenta de la Comisión Europea y Comisaria de Justicia, señalaba en una declaración hecha el 28 de enero de 2014 que el acuerdo de puerto seguro tenía que ser reforzado o sería suspendido *("Safe Harbour has to be strengthened or it will be suspended."*). Véase la declaración, en inglés, en http://europa.eu/rapid/press-release_SPEECH-14-62_es.htm

[78] Se trata del document titulado *Riga Statement on Enhancing transatlantic cooperation in the area of Freedom, Security and Justice*. Disponible, en inglés, en la dirección de Internet https://eu2015.lv/images/Kalendars/IeM/Riga_Statement_EU_US_Ministers.pdf

interminable[79], si bien en esta ocasión la Comisaria Jorouvá señaló[80] que se han alcanzado firmes compromisos sobre los aspectos comerciales y que se espera completar una revisión sólida del Marco del Puerto Seguro[81].

Más allá de la tensión política y de cuestiones que tienen que ser tratadas con atención específica[82], como ocurre con el acceso a los datos personales con fines de seguridad nacional, que no obstante están interrelacionadas en cierta medida con las relaciones comerciales así como con la garantía de la privacidad o la protección de datos personales, son muchas las razones por las que avanzar sobre el Acuerdo de Puerto Seguro es necesario, ya que de ello depende que las empresas, tanto las que exportan datos desde la Unión Europea como las que los importan en Estados Unidos, puedan beneficiarse de un mecanismo que resulta adecuado para impulsar la economía digital, con lo que ello supone para los consumidores que, además, son titulares de los datos personales que se tratan y que también encuentran un mecanismo de protección en dicho acuerdo.

Dilatar por más tiempo un acuerdo que es necesario e "inevitable", en el sentido de cualquier otro escenario sería inconcebible por las importantes implicaciones negativas que tendría en muchas áreas, se traduce en perjuicios para todas las partes y podría llegar a convertirse en un obstáculo para las relaciones comerciales, tener un impacto en la innovación, así como tener consecuencias a la hora de garantizar la protección de datos personales y la privacidad. Se trata de mucho más que un acuerdo, ya que poder llegar a un "puerto seguro" es necesario para construir sobre el mismo las bases de otros instrumentos que permitan ofrecer un mecanismo adecuado a otros socios comerciales, incluso comunes a la Unión Europea y a los Estados Unidos, alrededor del mundo con garantías para la protección de datos personales y la privacidad, que es también un interés común para los anteriores puesto que las empresas y las personas, sean clientes y/o titulares de un derecho fundamental, deben tener garantizada la seguridad jurídica necesaria para poder actuar con confianza.

Pensar en un nuevo Acuerdo que sustituya al actual y que sea el adecuado para perdurar en el tiempo sin fricciones, o en su caso con las menos posibles, es también una opción deseable. Y esto pasa, entre otros aspectos, por aclarar dudas que se han planteado durante los últimos años, por ejemplo, en cuanto a las transferencias ulteriores (en inglés, *"onward transfers"*), adoptar medidas que permitan una aproximación y aplicación homogénea por las autoridades de protección de datos y reforzar el cumplimiento para facilitar su aplicación.

---

[79] Cabe recordar que en la COM(2013) 846 final, la Comisión Europea indicaba que: *"Con carácter de urgencia, la Comisión debatirá con las autoridades de los Estados Unidos las deficiencias detectadas. Las soluciones deberán hallarse antes del final del verano de 2014 y aplicarse lo antes posible."* (pág. 8).

[80] Los puntos de prensa para la declaración de la Comisaria, tras el encuentro ya indicado, puede verse, en inglés, en http://ec.europa.eu/commission/2014-2019/jourova/announcements/press-speaking-points-commissioner-jourova-eu-us-justice-and-home--0_en

[81] En concreto, se indica que *"On Safe Harbour, with the Department of Commerce, we have achieved solid commitments on the commercial aspects. However, work still needs to continue as far as national security exemptions are concerned. Discussions will continue, with the aim of achieving a robust revision of the Safe Harbour framework in the near future."*

[82] Sobre la vigilancia de la Agencia de Seguridad Nacional de los EE.UU., véase, por ejemplo, el Informe de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo (A7-0139/2014), de 21 de febrero de 2014. Disponible en la dirección de Internet http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2014-0139+0+DOC+PDF+V0//ES

En definitiva, el resultado de este largo proceso de negociaciones deberá dar lugar a un Acuerdo de Puerto Seguro renovado y con vocación de perdurar en el tiempo. Aprovechar la experiencia acumulada e incidir en cuestiones tales como la transparencia de las prácticas de privacidad y protección de datos personales de las organizaciones adheridas al Puerto Seguro; el nivel de cumplimiento (en inglés, *"enforcement"*) del acuerdo, especialmente por la FTC, y reforzar la cooperación transatlántica, siguen siendo claves para impulsar la economía digital al mismo tiempo que se impulsa un alto nivel de garantía para la privacidad y el derecho fundamental a la protección de datos.