COMISIÓN
EUROPEA

Bruselas, 27.11.2013
COM(2013) 847 final

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

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

1. INTRODUCCIÓN

La Directiva 95/46/CE, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en lo sucesivo denominada «la Directiva sobre protección de datos») establece las normas para las transferencias de datos personales desde los Estados miembros de la UE a otros países terceros[1] en la medida en que tales transferencias están incluidas en el ámbito de aplicación de dicho instrumento[2].

En virtud de lo dispuesto en esa Directiva, la Comisión puede hacer constar que un país tercero garantiza un nivel de protección adecuado a la vista de su legislación interna o de los compromisos internacionales que haya suscrito a efectos de la protección de los derechos de las personas, en cuyo caso no se aplicarán las restricciones específicas a las transferencias de datos a dicho país. Estas decisiones se denominan normalmente **«decisiones de adecuación»**.

El 26 de Julio de 2000, la Comisión adoptó la Decisión 2000/520/CE[3] (en lo sucesivo denominada «**la Decisión de puerto seguro**»), en la que reconoce que los principios de puerto seguro para la protección de la vida privada (en lo sucesivo denominados «los principios») y las preguntas más frecuentes publicadas por el Departamento de Comercio de Estados Unidos ofrecen un nivel de protección adecuado a fines de la transferencia de datos personales desde la UE. La Decisión de puerto seguro se adoptó tras un dictamen del Grupo de trabajo del artículo 29 y de un dictamen del Comité del artículo 31 emitido por una mayoría cualificada de Estados miembros. De conformidad con la Decisión 1999/468 del Consejo, la Decisión de puerto seguro fue sometida al control previo del Parlamento Europeo.

Consecuentemente, la actual Decisión de puerto seguro permite la libre transferencia[4] de datos personales de los Estados miembros de la UE[5] a empresas en Estados Unidos que hayan suscrito los principios, en circunstancias que, de no ser así, no cumplirían las normas europeas para un nivel adecuado de protección de los datos, habida cuenta de las importantes diferencias existentes entre ambos lados del Atlántico respecto a los regímenes de protección de la vida privada.

El funcionamiento del actual marco de puerto seguro se basa en los compromisos y la autocertificación de las entidades que lo han suscrito. Si bien la firma de estos acuerdos es

---

1 Los artículos 25 y 26 de la Directiva sobre protección de datos establecen el marco jurídico para las transferencias de datos personales desde la UE a países terceros fuera del EEE.

2 El artículo 13 de la Decisión Marco 2008/977/JAI, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, establece normas adicionales en la medida en que tales transferencias se refieran a datos personales transmitidos, o puestos a disposición, por un Estado miembro a otro Estado miembro que tenga la intención de transferir esos datos posteriormente a terceros Estados u organismos internacionales con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o para la ejecución de sanciones penales.

3 Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América, DO 215 de 28.8.2000, p. 7.

4 Ello no excluye que se apliquen al tratamiento de los datos otras exigencias que puedan existir con arreglo a las legislaciones nacionales de aplicación de la Directiva de protección de datos.

5 Tras la ampliación de la Directiva 95/46/CE al Acuerdo sobre el EEE (Decisión 38/1999 de 25 de junio de 1999, DO L 296 de 23.11.2000, p. 41), las transferencias de datos procedentes de los tres Estados Parte del EEE funcionan de manera similar.

voluntaria, sus reglas son vinculantes para los que los suscriben. Los principios fundamentales de este tipo de acuerdos son:

a) la transparencia de las políticas de protección de la vida privada adoptadas por las entidades participantes,

b) la incorporación de los principios de puerto seguro a las políticas de protección de la vida privada adoptadas por las entidades, y,

c) la aplicación, en particular por parte de los poderes públicos.

Es necesario revisar la base fundamental del marco de puerto seguro en el **nuevo contexto** caracterizado por:

a) el aumento exponencial de flujos de datos que aunque anteriormente eran secundarios se han convertido en esenciales para el rápido crecimiento de la economía digital, y los notables avances en materia de recopilación, tratamiento y utilización de los datos,

b) la importancia fundamental de los flujos de datos, especialmente para la economía transatlántica[6],

c) el rápido crecimiento del número de empresas de Estados Unidos adheridas al marco de puerto seguro, que se ha multiplicado por ocho desde 2004 (pasando de 400 en 2004 a 3 246 en 2013),

d) las informaciones divulgadas recientemente sobre los programas de vigilancia estadounidenses, que plantea nuevas cuestiones acerca del nivel de protección que se supone debe garantizar el marco de puerto seguro.

En este contexto, la presente Comunicación hace balance del funcionamiento del marco de puerto seguro. **Se basa en datos** recopilados por la Comisión, los trabajos del Grupo de contacto UE-EE.UU. sobre protección de la vida privada llevados a cabo en 2009, un estudio elaborado por un contratista independiente en 2008[7] y la información recabada por el Grupo de trabajo *ad hoc* UE-EE.UU. (en lo sucesivo denominado el «Grupo de trabajo») creado a raíz de las revelaciones sobre los programas de vigilancia estadounidenses (véase el documento que se presenta paralelamente). La presente Comunicación constituye la continuación de los dos **informes de evaluación** elaborados por la **Comisión** en el periodo de puesta en marcha del marco de puerto seguro, 2002[8] y 2004[9] respectivamente.

2. ESTRUCTURA Y FUNCIONAMIENTO DEL PUERTO SEGURO

2.1. Estructura del puerto seguro

Una entidad estadounidense que desee adherirse al marco de puerto seguro deberá: a) indicar en su política de protección de la vida privada, accesible para el público, que suscribe los

6 Según algunos estudios, si los servicios y los flujos de datos transfronterizos se vieran perturbados porque dejasen de aplicarse las normas corporativas vinculantes, los modelos de cláusulas contractuales y el marco de puerto seguro, las repercusiones negativas sobre el PIB de la UE podrían ir de un -0,8 % a un -1,3 % y las exportaciones de servicios de la UE a Estados Unidos caerían en un -6,7 % debido a la pérdida de competitividad. Véase el estudio del Centro Europeo de Economía Política Internacional para la Cámara de Comercio estadounidense de marzo de 2013: *The Economic Importance of Getting Data Protection Right*.

7 Estudio de evaluación de impacto elaborado para la Comisión Europea en 2008 por el *Centre de Recherche Informatique et Droit* (CRID) de la Universidad de Namur.

8 Documento de trabajo de los servicios de la Comisión: *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 FAQs issued by the US Department of Commerce*, SEC (2002) 196 de 13.12.2002.

9 Documento de trabajo de los servicios de la Comisión: *The implementation of Commission Decision 520/2000/EC 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 20.10.2004.

principios y los cumple realmente y b) autocertificar su adhesión a los principios, es decir, notificar al Departamento de Comercio de Estados Unidos su conformidad con los mismos. La autocertificación debe renovarse cada año. Los principios de puerto seguro para la protección de la vida privada que se adjuntan en el anexo I de la Decisión de puerto seguro comprenden requisitos relativos tanto a la protección sustantiva de los datos personales (principios de integridad de los datos, seguridad, opción y transferencia ulterior) como a los derechos procedurales de los titulares de los datos (principios de notificación, acceso y aplicación).

Dos instituciones estadounidenses desempeñan un papel esencial en la aplicación del marco de puerto seguro en Estados Unidos: el Departamento de Comercio y la Comisión Federal de Comercio.

El **Departamento de Comercio** revisa todas las autocertificaciones de adhesión a los principios de puerto seguro y todas las cartas anuales de renovación enviadas por las entidades con el fin de garantizar que incluyen todos los elementos requeridos para la adhesión al marco[10]. Actualiza una lista de entidades que han presentado cartas de autocertificación y publica la lista y las cartas en su sitio *web*. Además, supervisa el funcionamiento del puerto seguro y elimina de la lista a las entidades que no cumplen sus principios.

La **Comisión Federal de Comercio**, dentro de sus atribuciones en materia de protección de los consumidores, interviene contra las prácticas desleales o fraudulentas de conformidad con el artículo 5 de la *Free Trade Commission Act*. Entre las medidas de aplicación que puede tomar, cabe citar la investigación de las declaraciones falsas de adhesión a los principios de puerto seguro y el incumplimiento de dichos principios por parte de entidades participantes. En el caso específico de la aplicación de los principios de puerto seguro a las compañías aéreas, el órgano competente es el Departamento de Transporte de Estados Unidos[11].

La actual Decisión de puerto seguro forma parte de la legislación de la UE que debe ser aplicada por las autoridades de los Estados miembros. En virtud de dicha Decisión, en casos específicos las **autoridades nacionales de protección de datos** de la UE están facultadas para suspender las transferencias de datos a una entidad que haya certificado su adhesión a los principios de puerto seguro[12]. Desde la creación del marco de puerto seguro en el año 2000, la Comisión no ha tenido conocimiento de ningún caso de suspensión por parte de una autoridad nacional de protección de datos. Independientemente de las facultades que les otorga la Decisión de puerto seguro, dichas autoridades nacionales están facultadas para intervenir, incluso en caso de transferencias internacionales, a fin de garantizar el cumplimiento de los principios generales en materia de protección de datos expuestos en la Directiva de protección de datos de 1995.

Como recuerda la Decisión de puerto seguro, **corresponde a la Comisión,** de acuerdo con el procedimiento de examen expuesto en el Reglamento nº 182/2011, adaptar la Decisión, suspenderla o limitar su ámbito de aplicación en cualquier momento, de conformidad con la

---

10 Si la certificación o la renovación de la certificación de una entidad no cumple los requisitos de puerto seguro, el Departamento de Comercio comunicará a dicha entidad los pasos que deba dar (por ejemplo, aclaraciones o modificaciones en la descripción de su política) antes de que pueda completarse su procedimiento de certificación.

11 De conformidad con el título 49, § 41712 del US Code.

12 Más concretamente, puede pedirse la suspensión de las transferencias en dos situaciones, cuando:
a) el organismo público de Estados Unidos haya resuelto que la entidad está vulnerando los principios de puerto seguro para la protección de la vida privada;
b) existan grandes probabilidades de que se estén vulnerando los principios de puerto seguro; exista un motivo razonable para creer que el mecanismo de aplicación correspondiente no está tomando o no tomará las medidas oportunas para resolver el caso en cuestión; la continuación de la transferencia podría crear un riesgo inminente de grave perjuicio a los afectados; y las autoridades competentes del Estado miembro hayan hecho esfuerzos razonables, dadas las circunstancias, para notificárselo a la entidad y darle la oportunidad de presentar sus alegaciones.

experiencia resultante de su aplicación. Así está previsto especialmente si se da un incumplimiento sistemático por parte estadounidense, por ejemplo, si un órgano responsable de velar por el cumplimiento de los principios de puerto seguro en Estados Unidos no está cumpliendo su función de manera efectiva, o si el nivel de protección que ofrecen los principios de puerto seguro es superado por los requisitos de la legislación estadounidense. Al igual que todas las decisiones de la Comisión, la Decisión de puerto seguro también puede ser modificada, o incluso derogada, por otros motivos.

2.2. Funcionamiento del marco de puerto seguro

Entre las **3 246 entidades certificadas**[13] las hay tanto grandes como pequeñas[14]. Aunque los servicios financieros y las industrias de telecomunicación no están sujetos a las competencias de ejecución de la Comisión Federal de Comercio y, por tanto, están excluidos del marco de puerto seguro, entre las entidades certificadas hay muchas industrias y sectores de servicios, entre ellos empresas de internet muy conocidas e industrias que van desde servicios de información e informática a farmacéuticas, servicios de viaje y turismo, servicios de asistencia sanitaria o servicios de tarjetas de crédito[15]. Se trata fundamentalmente de entidades estadounidenses que ofrecen servicios en el mercado interior de la UE. Hay también filiales de algunas empresas de la UE, como Nokia o Bayer. El 51 % son empresas que, para la gestión de sus recursos humanos, transfieren a Estados Unidos datos de sus empleados europeos[16].

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.

El actual marco de puerto seguro se basa en la adhesión voluntaria de las entidades, en la autocertificación de las mismas y en la aplicación de los compromisos de autocertificación por parte de las autoridades públicas. En este contexto, cualquier falta de transparencia y cualquier deficiencia en la aplicación socavan los cimientos que sustentan el marco.

Cualquier fallo en la transparencia o en la aplicación por parte estadounidense hace que la responsabilidad pase a las autoridades de protección de datos y las empresas europeas que utilizan el sistema. El 29 de abril de 2010 las autoridades de protección de datos alemanas publicaron una decisión en la que pedían a las entidades que transfieren datos de Europa a Estados Unidos que comprobasen si las entidades estadounidenses que importaban los datos cumplían realmente los principios de puerto seguro y recomendaban que «al menos la empresa exportadora debe comprobar si la certificación de puerto seguro del importador sigue siendo válida»[17].

---

13 A 26 de septiembre de 2013, el número de entidades que figuraban en la lista de puerto seguro como «**actualizadas**» era **3 246,** y el de entidades con certificación «**no actualizada**» era **935.**

14 Entidades adheridas a los principios de puerto seguro con 250 empleados o menos: **60 %** (1 925 de 3 246); con al menos 251 empleados: **40 %** (1 295 de 3 246).

15 MasterCard, por ejemplo, trata con miles de bancos y constituye un claro ejemplo de situación en la que no es posible remplazar el marco de puerto seguro por otros instrumentos legales para las transferencias de datos personales, como normas corporativas vinculantes o acuerdos contractuales.

16 Organizaciones adheridas al puerto seguro que gestionan sus datos sobre recursos humanos en virtud de su certificación (y que, por tanto, han expresado su acuerdo para cooperar y cumplir lo dispuesto por las autoridades de protección de datos de la UE): **51 %** (1 671 de 3 246).

17 Véase la decisión Düsseldorfer Kreis de 28/29 de abril de 2010. *Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich* de 28/29 de abril 2010, Hannover: http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DuesseldorferKreis/290410_SafeHarbor.pdf?__bl

El 24 de julio de 2013, a raíz de las revelaciones sobre los programas estadounidenses de vigilancia, las autoridades de protección de datos alemanas fueron más allá y manifestaron su inquietud afirmando que existía una gran probabilidad de que se estuvieran infringiendo los principios de las decisiones de la Comisión[18]. Algunas de ellas (por ejemplo, la de Bremen) han pedido a las empresas que transfieren datos personales a proveedores estadounidenses que les comuniquen si dichos proveedores impiden a la Agencia Nacional de Seguridad estadounidense el acceso a los datos, y cómo lo hacen. La agencia irlandesa de protección de datos comunicó que había recibido recientemente dos quejas referentes al marco de puerto seguro a raíz de la información sobre los programas de las agencias de inteligencia estadounidenses, aunque había decidido no investigarlas porque la transferencia de datos personales a un tercer país satisface las exigencias de la legislación irlandesa en la materia. Tras haber recibido una queja similar, la autoridad de protección de datos de Luxemburgo llegó a la conclusión de que Microsoft y Skype habían cumplido la legislación luxemburguesa sobre protección de datos al transferir datos a Estados Unidos[19]. No obstante, el Tribunal Supremo de Irlanda ha admitido a trámite una solicitud de control jurisdiccional en virtud de la cual examinará la inacción del Comisario de Protección de Datos irlandés en relación con los programas de vigilancia estadounidenses. Una de las dos denuncias fue presentada por un grupo de estudiantes, *Europe v Facebook* (EvF), que había presentado una denuncia similar contra Yahoo en Alemania que está siendo tramitada por las autoridades de protección de datos correspondientes.

Estas respuestas divergentes de las autoridades de protección de datos ante las revelaciones en torno a los programas de vigilancia demuestran que existe un riesgo real de fragmentación del marco de puerto seguro y plantean cuestiones sobre el grado en que se aplica.

3. TRANSPARENCIA DE LAS POLÍTICAS DE PROTECCIÓN DE LA VIDA PRIVADA DE LAS ENTIDADES PARTICIPANTES

Según la pregunta más frecuente nº 6 anexa a la Decisión de puerto seguro (anexo II), las entidades interesadas en certificar su adhesión a los principios de puerto seguro tienen que facilitar al Departamento de Comercio su política de protección de la vida privada y hacerla pública, incluyendo su compromiso de adherirse a los principios. El requisito de **hacer públicas las políticas de protección de la vida privada** de las entidades autocertificadas, al igual que su declaración de adhesión a los principios de privacidad, son fundamentales para el funcionamiento del sistema.

Un acceso insuficiente a las políticas de protección de la vida privada de dichas entidades perjudica a los particulares cuyos datos personales se estén recopilando y tratando, pudiendo constituir una **infracción del principio de notificación**. En tales casos es posible que los particulares cuyos datos se estén transfiriendo desde la UE no sean conscientes de sus derechos ni de las obligaciones a que está sujeta una entidad autocertificada.

Por otra parte, el compromiso de las entidades de cumplir los principios de protección de la vida privada **otorga competencias a la Comisión Federal de Comercio para actuar** contra ellas en caso de incumplimiento que dé lugar a prácticas desleales o fraudulentas. La falta de

---

ob=publicationFile. Sin embargo, el 7 de octubre de 2013 el Supervisor Europeo de Protección de Datos, Peter Hustinx, manifestó en la investigación de la Comisión LIBE del Parlamento Europeo que se habían conseguido mejoras sustanciales y ya se habían solucionado la mayor parte de los problemas en lo que respecta al puerto seguro: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-10-07_Speech_LIBE_PH_EN.pdf

18 Véase la resolución de la Conferencia alemana de comisarios encargados de la protección de datos en la que se pone de relieve que los servicios de inteligencia constituyen una amenaza importante para el tráfico de datos entre Alemania y los países de fuera de Europa: http://www.bfdi.bund.de/EN/Home/homepage_Kurzmeldungen/PMDSK_SafeHarbor.html?nn=408870

19 Véase el comunicado de prensa de la autoridad de protección de datos de Luxemburgo de 18 de noviembre de 2013.

transparencia de las entidades estadounidenses dificulta la supervisión de la Comisión Federal de Comercio y socava la eficacia de la aplicación.

A lo largo de los años, un número importante de entidades autocertificadas no han hecho pública su política de protección de la vida privada o no han declarado públicamente su adhesión a los principios de puerto seguro. El informe de puerto seguro de 2004 señalaba la necesidad de que el Departamento de Comercio **se muestre más activo en el control del cumplimiento** de este requisito.

Desde 2004 el Departamento de Comercio ha desarrollado **nuevas herramientas de información** para ayudar a las entidades a cumplir sus obligaciones en materia de transparencia. El Departamento de Comercio tiene un sitio *web* dedicado al marco de puerto seguro[20] en el que las entidades pueden cargar sus políticas de protección de la vida privada. Según el Departamento de Comercio, cuando una entidad solicita adherirse al marco de puerto seguro utiliza esta opción y carga su política de protección de la vida privada en el sitio[21]. Asimismo, entre 2009 y 2013 el Departamento de Comercio ha publicado una serie de directrices para las entidades que deseen participar, como una guía y consejos para la autocertificación (*Guide to Self-Certification* y *Helpful Hints on Self-Certifying Compliance*)[22].

El grado de cumplimiento de las obligaciones de transparencia varía en función de las distintas entidades. Mientras que algunas se limitan a transmitir al Departamento de Comercio una descripción de su política de protección de la vida privada, como parte del procedimiento de autocertificación, la mayoría publica dichas políticas en sus sitios además de cargarlas en el sitio *web* del Departamento de Comercio. No obstante, **dichas políticas no siempre se presentan de forma que facilite la lectura y sea comprensible para los consumidores**. Los hipervínculos a las políticas de protección de la vida privada a veces no funcionan correctamente ni remiten a las páginas *web* correspondientes.

De la Decisión y sus anexos se desprende que la exigencia de que las entidades hagan públicas sus políticas de protección de la vida privada **va más allá de la mera notificación** de la autocertificación al Departamento de Comercio. Los requisitos de certificación expuestos en las preguntas más frecuentes incluyen una descripción de la política de protección de la vida privada, así como información sobre el lugar donde puede consultarla el público[23]. Las declaraciones relativas a su política de protección de la vida privada tienen que ser claras y de fácil acceso para el público. Deben incluir un hipervínculo a la página *web* de puerto seguro del Departamento de Comercio que contiene una lista de todos los miembros «actualizados» del régimen, así como un vínculo que reenvíe a la instancia de solución extrajudicial de litigios. Ahora bien, varias entidades adheridas al régimen en el período 2000-2013 no cumplían estos requisitos. En sus contactos con la Comisión en febrero de 2013, el Departamento de Comercio reconoció la posibilidad de que hasta un 10 % de las entidades certificadas no hayan incluido en sus respectivos sitios *web* públicos su política de protección de la vida privada, incluyendo una declaración de adhesión al marco de puerto seguro.

Asimismo, las estadísticas más recientes ponen de manifiesto un problema persistente de **alegaciones falsas de adhesión al puerto seguro**. En torno a un 10 % de las entidades que

20 http://www.export.gov/SafeHarbour/.

21 https://SafeHarbour.export.gov/list.aspx.

22 La Guía está disponible en el sitio *web* del programa: http://export.gov/SafeHarbour/ Helpful Hints: http://export.gov/SafeHarbour/eu/eg_main_018495.asp.

23 El 12 de noviembre de 2013 el Departamento de Comercio confirmó que actualmente las entidades que tienen sitios *web* públicos y tratan datos relativos a consumidores, clientes o visitantes deben incluir en ellos su política de protección de la vida privada con arreglo al marco de puerto seguro (documento: *U.S.-EU Cooperation to Implement the Safe Harbor Framework* de 12 de noviembre de 2013).

afirman ser miembros de este marco no figuran en la lista de miembros actuales del Departamento de Comercio[24]. Tales afirmaciones falsas proceden tanto de entidades que nunca han participado en el marco de puerto seguro como de entidades que se habían adherido a él, pero posteriormente no enviaron la renovación anual de su autocertificación al Departamento de Comercio. En tal caso, siguen figurando en el sitio *web* de puerto seguro, pero con un estatus de certificación «no actualizado», lo que significa que la entidad ha sido miembro del régimen, por lo que tiene la obligación de seguir ofreciendo protección a los datos ya tratados. La Comisión Federal de Comercio está facultada para intervenir en caso de prácticas fraudulentas e incumplimiento de los principios de puerto seguro (véase el punto 5.1). La falta de claridad en torno a las «alegaciones falsas» perjudica a la credibilidad del sistema.

En sus contactos regulares a lo largo de 2012 y 2013 la Comisión Europea advirtió al Departamento de Comercio que, para cumplir las obligaciones en materia de transparencia, no basta con que las empresas se limiten a facilitarle una descripción de su política de protección de la vida privada; dicha política debe ponerse a disposición del público. Asimismo le pidió que **intensificara sus controles periódicos de los sitios *web* de las entidades** tras haber llevado a cabo el procedimiento de verificación en el contexto del primer procedimiento de autocertificación o de su renovación anual, y que emprendiera acciones contras las que incumplieran los requisitos en materia de transparencia.

Como primera respuesta a las inquietudes expresadas por la UE, **desde marzo de 2013 el Departamento de Comercio obliga** a las entidades adheridas al puerto seguro que tengan un sitio *web* público a incluir en el mismo su política de protección de la vida privada en lo que respecta a los datos de sus clientes o usuarios. Al mismo tiempo, empezó a notificar a las entidades cuya política de protección de la vida privada no incluía todavía un vínculo al sitio *web* de puerto seguro del Departamento de Comercio que debían incluirlo, con el fin de que los consumidores que visiten el sitio *web* de una entidad puedan acceder directamente a él. Ello permitirá a los ciudadanos europeos cuyos datos se difundan comprobar inmediatamente en el sitio *web* de una entidad, sin necesidad de efectuar más búsquedas, los compromisos presentados por dicha entidad al Departamento de Comercio. Además, el Departamento de Comercio ha comenzado a notificar a las entidades que la información sobre su política de protección de la vida privada que figura en su sitio *web* debe incluir los datos de la instancia independiente para la resolución de litigios[25].

Conviene acelerar este proceso para garantizar que todas las entidades certificadas cumplan plenamente los requisitos de puerto seguro a más tardar en marzo de 2014 (es decir, en el plazo para la renovación de la certificación de las entidades contado a partir de la introducción de los nuevos requisitos en marzo de 2013).

No obstante, todavía no está claro si todas las entidades autocertificadas satisfacen plenamente las exigencias en materia de transparencia. El Departamento de Comercio debe supervisar e investigar con mayor rigor el cumplimiento de las obligaciones asumidas en el momento de la autocertificación inicial y de su renovación anual.

---

24 En septiembre de 2013 la empresa australiana de consultoría Galexia comparó las «alegaciones falsas» de adhesión al puerto seguro en 2008 y 2013. Su principal conclusión fue que, paralelamente al incremento del número de miembros de puerto seguro entre 2008 y 2013 (de 1 109 a 3 246), el número de alegaciones falsas pasó de 206 a 427. http://www.galexia.com/public/about/news/about_news-id225.html .

25 Entre marzo y septiembre de 2013 el Departamento de Comercio ha:
• notificado a las 101 entidades *que ya habían colgado su política de protección de la vida privada en el sitio* web *del puerto seguro* que debían colgar asimismo dicha política en el sitio de su entidad;
• notificado a las 154 entidades que todavía no lo habían hecho que debían incluir un enlace al sitio *web* de puerto seguro en su política de protección de la vida privada;
• notificado a más de 600 entidades que debían incluir en su política de protección de la vida privada los datos de la instancia independiente para la resolución de litigios.

4. INTEGRACIÓN DE LOS PRINCIPIOS DE PUERTO SEGURO EN LAS POLÍTICAS DE LAS ENTIDADES PARA LA PROTECCIÓN DE LA VIDA PRIVADA

Para obtener y mantener las ventajas que confiere el marco de puerto seguro, las entidades autocertificadas deben cumplir los principios de protección de la vida privada que figuran en el anexo I de la Decisión.

En su informe de 2004 la Comisión constató que un número importante de **entidades no habían incorporado correctamente los principios de puerto seguro para la protección de la vida privada** a sus políticas sobre tratamiento de datos. Por ejemplo, no siempre facilitaban a los particulares información clara y transparente sobre los fines para los que se trataban sus datos, o no les ofrecían la opción de decidir (exclusión) si sus datos podían transmitirse a un tercero o utilizarse para un fin incompatible con el objetivo inicial con que se habían recogido. El informe de la Comisión de 2004 consideraba que el Departamento de Comercio debería actuar con más determinación en lo que respecta al acceso al marco de puerto seguro y a la concienciación sobre sus principios[26].

Los progresos a este respecto han sido limitados. Desde el 1 de enero de 2009 el Departamento de Comercio evalúa la política de protección de la vida privada antes de renovar la certificación de puerto seguro de las entidades que deseen hacerlo – lo que debe hacerse anualmente. Sin embargo, es una evaluación limitada, ya que **no se evalúan plenamente las prácticas reales** de las entidades autocertificadas, lo que haría mucho más fiable el procedimiento de autocertificación.

Tras pedir la Comisión al Departamento de Comercio que supervisase de manera más rigurosa y sistemática a las entidades autocertificadas, **las nuevas solicitudes se están examinando con mayor atención**. El número de nuevas solicitudes rechazadas que se devuelven a las entidades para que mejoren sus políticas de protección de la vida privada ha aumentado significativamente entre 2010 y 2013: se ha duplicado para las entidades que desean renovar su certificación y se ha triplicado para las que desean adherirse al marco de puerto seguro por primera vez[27]. El Departamento de Comercio ha garantizado a la Comisión que las certificaciones, o las renovaciones de las mismas, solo podrán llevarse a cabo si la política de protección de datos de la entidad satisface todos los requisitos, especialmente incluir el compromiso de adhesión a los principios pertinentes de puerto seguro y ser accesible al público. En su registro en la lista de puerto seguro, las entidades deben indicar la ubicación de su política. Asimismo tienen que indicar claramente en su sitio *web* una instancia independiente de resolución de litigios e incluir un vínculo al sitio de puerto seguro en la *web* del Departamento de Comercio. Sin embargo, se estima que más del 30 % de los miembros de puerto seguro no incluyen información sobre resolución de litigios en las políticas de privacidad que figuran en sus sitios *web*[28].

La mayoría de las entidades retiradas de la lista de puerto seguro por el Departamento de Comercio lo fueron por petición propia (por ejemplo, entidades fusionadas o adquiridas por otras, que han cambiado su línea de negocio o que han cesado sus actividades). Asimismo se ha eliminado un número más reducido de entidades extinguidas, cuando sus sitios *web*

---

26 Véase la página 8 del Informe de 2004, SEC (2004) 1323.

27 Según las estadísticas presentadas en septiembre de 2013 por el Departamento de Comercio, en 2010 el Departamento notificó a un 18 % (93) de las 512 entidades que pedían la certificación por primera vez y a un 16 % (231) de las 1 417 que deseaban renovarla que debían mejorar sus políticas de protección de la vida privada o sus solicitudes de adhesión al marco de puerto seguro. En cambio, tras la petición de la Comisión de una vigilancia más estricta, diligente y sistemática de todas las solicitudes, a mediados de septiembre de 2013 el Departamento había notificado a un 56 % (340) de las 602 entidades que pedían la certificación por primera vez y a un 27 % (493) de las 1 809 que deseaban renovarla que debían mejorar sus políticas de protección de la vida privada.

28 Comparecencia de Chris Connolly (Galexia) ante la investigación de la Comisión LIBE del Parlamento Europeo el 7 de octubre de 2013.

incluidos en los registros ya no estaban operativos y su certificación llevaba varios años sin renovarse[29]. Es importante señalar que no parece haberse retirado de la lista ninguna entidad debido a problemas de cumplimiento detectados en la verificación del Departamento de Comercio.

La lista de puerto seguro es a la vez el anuncio público de que una entidad se ha adherido al marco y un registro de los compromisos de puerto seguro suscritos. **El compromiso de adherirse a los principios de puerto seguro es de duración ilimitada** en lo que respecta a los datos recibidos durante el periodo en que la entidad se beneficia del marco, y dicha entidad debe seguir aplicando los principios a esos datos durante todo el tiempo en que los almacene, utilice o divulgue, aunque haya abandonado el marco por algún motivo.

El número de **solicitantes que no superaron el examen administrativo** del Departamento de Comercio y, por tanto, no fueron incluidos en la lista de puerto seguro, es el siguiente: **en 2010** solo un **6 %** (33) de las 513 entidades que solicitaron adherirse por primera vez no fue incluido por no satisfacer las normas de autocertificación del Departamento; en **2013 no lo fue un 12%** (75) de las 605 entidades que lo solicitaron.

Como requisito mínimo para hacer más transparente su supervisión, el Departamento de Comercio debería incluir en su sitio *web* una lista de todas las entidades retiradas del marco de puerto seguro indicando los motivos por los que no se ha renovado su certificación. La indicación «sin actualizar» en la lista de miembros de puerto seguro del Departamento no debe considerarse una mera información, sino que debe ir acompañada de una **advertencia clara** – tanto gráfica como verbal – de que actualmente esa entidad no satisface los requisitos de puerto seguro.

Por otra parte, algunas entidades todavía no han incorporado todos los principios de puerto seguro. Además de los problemas de transparencia mencionados en la sección 3, a menudo las políticas de protección de la vida privada de las entidades autocertificadas no son claras en lo que respecta a los fines para los que recogen los datos y al derecho a decidir si dichos datos pueden transmitirse a terceras partes, lo que plantea dudas sobre el cumplimiento de los principios de «Notificación» y «Opción». Ambos principios son cruciales para garantizar a los titulares de los datos el control sobre sus datos personales.

No se garantiza suficientemente el primer paso crítico del proceso, a saber, la incorporación de los principios de puerto seguro a las políticas de protección de la vida privada de las entidades. El Departamento de Comercio debería solucionar este aspecto con carácter prioritario, elaborando una metodología a efectos del cumplimiento en las prácticas operacionales de las entidades y su interacción con los clientes. **El Departamento de Comercio deber realizar un seguimiento activo de la incorporación efectiva de los principios de puerto seguro a las políticas de privacidad de las entidades**, en vez de dejar que sean las quejas de los particulares las que den lugar a medidas de ejecución.

5. APLICACIÓN POR PARTE DE LAS AUTORIDADES PÚBLICAS

Existen diversos mecanismos que garantizan la aplicación efectiva del marco de puerto seguro y ofrecen una vía de recurso a los particulares cuando la protección de sus datos personales se vea afectada por el incumplimiento de los principios de protección de la vida privada.

Según el principio de «Aplicación», las políticas de las entidades autocertificadas en materia de vida privada deben incluir mecanismos efectivos para garantizar la conformidad con los

[29] A diciembre de 2011 el Departamento de Comercio estadounidense había eliminado 323 entidades de la lista de puerto seguro: 94 porque habían cesado sus actividades; 88 por motivos de adquisición o fusión, 95 a petición de la sociedad matriz; 41 porque llevaban varios años sin renovar su certificación y 5 por otros motivos.

principios. Como se explica más detalladamente en las preguntas más frecuentes números 11, 5 y 6, con arreglo al principio de «Aplicación» este requisito puede cumplirse mediante la adhesión a una **instancia independiente de recurso** cuya competencia para investigar las quejas de los particulares por incumplimiento de los principios haya sido reconocida públicamente. Otra alternativa es el compromiso de la entidad de cooperar con el **Grupo de expertos de la UE en protección de datos**[30]. Por otra parte, las entidades autocertificadas están sujetas a la jurisdicción de la Comisión Federal de Comercio a tenor de lo dispuesto en el artículo 5 de la Ley de la Comisión Federal de Comercio, que prohíbe los actos o prácticas desleales o fraudulentos en el comercio o en relación con él[31].

En el Informe de 2004 se exponían dudas sobre la aplicación del marco de puerto seguro y se afirmaba que la Comisión Federal de Comercio debería mostrarse más activa a la hora de abrir investigaciones y dar a conocer sus derechos a los particulares. Otra cuestión que suscitaba inquietudes era que no quedaba clara la competencia de dicha Comisión para aplicar los principios en lo que respecta a los datos sobre recursos humanos.

El órgano de recurso responsable cuando se trata de datos sobre recursos humanos, a saber, el Grupo de expertos de la UE en protección de datos, ha recibido una queja referente a este tema[32]. Ahora bien, la ausencia de quejas no permite extraer conclusiones sobre todo el funcionamiento del marco. Conviene llevar a cabo comprobaciones de oficio del cumplimiento por parte de las entidades a fin de verificar la aplicación real de los compromisos en materia de protección de datos. Asimismo, las autoridades de protección de datos de la UE deben emprender acciones para dar a conocer la existencia del Grupo de expertos.

Se han señalado problemas en relación con la forma en que los mecanismos de recurso extrajudicial funcionan como órganos de aplicación; varios de ellos carecen de los medios adecuados para poner remedio a los casos de incumplimiento de los principios, y hay que solucionar esta deficiencia.

5.1. Comisión Federal de Comercio

La Comisión Federal de Comercio puede tomar medidas de aplicación en caso de infracción de los compromisos de puerto seguro por parte de una entidad. Cuando se creó el marco de puerto seguro, la Comisión Federal se comprometió a tramitar con carácter prioritario todos los casos presentados por las autoridades de los Estados miembros de la UE[33]. Puesto que en los primeros diez años del sistema no se recibieron quejas, la Comisión Federal decidió buscar infracciones del puerto seguro en todas sus investigaciones sobre la protección de la vida privada y la seguridad de los datos. Desde 2009 ha puesto en marcha diez acciones de ejecución basadas en este tipo de infracciones, que han dado lugar a órdenes de liquidación – sujetas a sanciones importantes – por declaraciones falsas en materia de defensa de la vida

30 El Grupo de expertos de la UE en protección de datos es un órgano competente para investigar y resolver las quejas presentadas por los particulares por la supuesta infracción de los principios de puerto seguro por parte de una entidad estadounidense perteneciente al mismo. Las entidades que han certificado su cumplimiento de estos principios deben elegir entre adherirse a una instancia independiente de recurso o cooperar con el Grupo de expertos de la UE, a fin de solucionar los problemas derivados del incumplimiento de los principios de puerto seguro. No obstante, la cooperación con el Grupo de expertos de la UE es obligatoria cuando la entidad estadounidense trata datos personales sobre recursos humanos transferidos desde la UE para su uso en el contexto de la relación laboral. Si la entidad se compromete a cooperar con el Grupo de expertos de la UE, deberá comprometerse también a cumplir sus recomendaciones cuando el Grupo considere que la entidad debe tomar medidas concretas para cumplir los principios de puerto seguro, lo que incluye las indemnizaciones o compensaciones.

31 El Departamento de Transporte ejerce una jurisdicción similar sobre las compañías aéreas de conformidad con el USC, título 49, § 41712.

32 Se trata de una queja presentada por un ciudadano suizo, por lo que el Grupo de expertos de la UE la ha remitido a la autoridad suiza de protección de datos (Estados Unidos dispone de un marco independiente de puerto seguro para Suiza).

33 Véase el anexo V de la Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000.

privada, incluido el incumplimiento de los principios de puerto seguro, y a la imposición a las entidades de programas y auditorias en materia de privacidad durante veinte años. A petición de la Comisión Federal, las entidades deben aceptar evaluaciones independientes de sus programas de protección de la vida privada, que se transmiten regularmente a la Comisión Federal. Asimismo la Comisión Federal prohíbe a estas entidades presentar declaraciones falsas en lo que concierne a sus prácticas en materia de privacidad y a su participación en el puerto seguro o en otros marcos similares. Así sucedió, por ejemplo, en las investigaciones de la Comisión Federal contra Google, Facebook y Myspace[34]. En 2012 Google aceptó pagar una multa de 22,5 millones USD para que se retirara la acusación de que había infringido una orden de consentimiento. En todas sus investigaciones en materia de protección de la vida privada la Comisión Federal analiza de oficio si existe una infracción de los principios de puerto seguro.

La Comisión Federal de Comercio ha reiterado recientemente sus declaraciones y su compromiso de tramitar con carácter prioritario todos los casos presentados por entidades autorreguladas y por los Estados miembros de la UE referentes al incumplimiento de los principios de puerto seguro[35]. En los últimos tres años, las autoridades europeas de protección de datos solo han enviado unos pocos casos a la Comisión Federal.

La cooperación transatlántica entre autoridades de protección de datos ha empezado a desarrollarse recientemente. Por ejemplo, el 26 de junio de 2013 la Comisión Federal firmó un memorando de acuerdo con la Oficina del Comisario de Protección de Datos de Irlanda sobre asistencia mutua en la aplicación de las leyes de protección de datos personales en el sector privado. Este memorando establece un marco para incrementar, racionalizar y hacer más efectiva la cooperación en materia de respeto de la intimidad[36].

En agosto de 2013 la Comisión Federal anunció que iba a intensificar las comprobaciones de las entidades que controlan grandes bases de datos personales. También ha creado un portal en el que los consumidores pueden presentar sus quejas sobre el respeto de la intimidad por parte de una entidad estadounidense[37].

Asimismo, la Comisión Federal debe incrementar sus esfuerzos para investigar las afirmaciones falsas de adhesión a puerto seguro. Una entidad que afirme en su sitio *web* que cumple los requisitos de puerto seguro, pero que no esté incluida en la lista del Departamento de Comercio como miembro «actualizado» de este marco está engañando a los consumidores y abusando de su confianza. Las afirmaciones falsas perjudican la credibilidad del sistema en su conjunto, por lo que deben ser retiradas inmediatamente de los sitios *web* de las entidades. Habría que imponer a las entidades la obligación de no inducir a error a los consumidores. La Comisión Federal debe seguir detectando las afirmaciones falsas de adhesión a puerto seguro, como en el asunto *Karnani*, cuando cerró un sitio *web* de California por afirmar

---

34 En el período 2009-2012 la Comisión Federal de Comercio ha finalizado diez medidas de ejecución relativas a compromisos de puerto seguro: FTC v. Javian Karnani, and Balls of Kryptonite, LLC (2009), World Innovators, Inc. (2009), Expat Edge Partners, LLC (2009), Onyx Graphics, Inc. (2009), Directors Desk LLC (2009), Progressive Gaitways LLC (2009), Collectify LLC (2009), Google Inc. (2011), Facebook, Inc. (2011), Myspace LLC (2012). Véase: *Federal Trade Commission of Safe Harbour Commitments*: http://export.gov/build/groups/public/@eg_main/@SafeHarbour/documents/webcontent/eg_main_052211.pdf. Véase también: *Case Highlights*: http://business.ftc.gov/us-eu-Safe-Harbour-framework. La mayoría de estos casos se referían a problemas con entidades que se habían adherido en el pasado al marco de puerto seguro pero que, a pesar de no haber renovado su certificación anual, seguían presentándose como miembros de dicho marco.

35 Este compromiso se reiteró en una reunión de la comisaria de la Comisión Federal de Comercio, Julie Brill, con las autoridades de protección de datos de la UE (Grupo de trabajo del artículo 29) en Bruselas el 17 de abril de 2013.

36 http://www.dataprotection.ie/viewdoc.asp?Docid=1317&Catid=66&StartDate=1+January+2013&m=n

37 Los consumidores pueden presentar sus quejas a través del Asistente de Quejas FTC (https://www.ftccomplaintassistant.gov/) y los consumidores extranjeros pueden hacerlo a través de econsumer.gov (http://www.econsumer.gov .

engañosamente su inscripción en puerto seguro y llevar a cabo prácticas comerciales en línea fraudulentas dirigidas a los consumidores europeos[38].

El 29 de octubre de 2013 la Comisión Federal anunció que había puesto en marcha «numerosas investigaciones en relación con el cumplimiento de los principios de puerto seguro en los últimos meses» y que cabía esperar más medidas de ejecución en este frente «en los meses venideros». Asimismo confirmó que se había «comprometido a buscar formas de mejorar su eficacia» y que «continuaría agradeciendo todas las pistas interesantes, como la queja recibida en los últimos meses de un defensor de los consumidores de Europa en la que alegaba un gran número de infracciones en relación con el puerto seguro»[39]. También se comprometió a «controlar sistemáticamente el cumplimiento de las instrucciones de puerto seguro, como lo hacemos con todas nuestras instrucciones»[40].

El 12 de noviembre de 2013, la Comisión Federal comunicó a la Comisión Europea que **«si una entidad, en su política de protección de la vida privada, garantiza protección de puerto seguro, el hecho de que dicha entidad no se inscriba o no mantenga su inscripción no basta por sí solo para evitar que la Comisión Federal de Comercio la obligue a cumplir sus compromisos de puerto seguro»**[41].

En noviembre de 2013 el Departamento de Comercio comunicó a la Comisión Europea que, «para ayudar a garantizar que las entidades no efectúan "afirmaciones falsas" sobre su participación en puerto seguro, el Departamento de Comercio empezará a ponerse en contacto con los participantes en puerto seguro un mes antes de la fecha en que deban renovar su certificación a fin de indicarles los pasos que deben seguir si decidieran no renovarla». **El Departamento de Comercio «comunicará a estas entidades** que deben retirar todas las referencias a su participación en puerto seguro, incluida la utilización de la marca de certificación de puerto seguro, de sus políticas de defensa de la vida privada y de sus sitios *web*, **y les notificará claramente que en caso de no hacerlo la Comisión Federal de Comercio podría emprender acciones contra ellas»**[42].

Para luchar las alegaciones falsas de adhesión a puerto seguro, las políticas de protección de la vida privada que aparecen en los sitios *web* de las entidades autocertificadas deberán incluir siempre un vínculo al sitio *web* de puerto seguro en el Departamento de Comercio, en el que figura una lista de todos los miembros «actualizados» del sistema. Ello permitirá a los titulares europeos de datos verificar inmediatamente, sin necesidad de más búsquedas, si una entidad es miembro de puerto seguro. En marzo de 2013 el Departamento de Comercio empezó a exigir este requisito a las entidades, pero es necesario intensificar el proceso.

El control permanente, y la aplicación consiguiente por la Comisión Federal, del cumplimiento real de los principios de puerto seguro – además de las medidas adoptadas por el Departamento de Comercio indicadas más arriba – siguen siendo una prioridad clave para garantizar el funcionamiento adecuado y efectivo del sistema. Es necesario, en particular, un número mayor de **investigaciones y comprobaciones de oficio del respeto de los principios de puerto seguro por parte de las entidades**. Asimismo, debe simplificarse el proceso de presentación de quejas por infracción a la Comisión Federal.

38 http://www.ftc.gov/os/caselist/0923081/090806karnanicmpt.pdf

39 http://www.ftc.gov/speeches/brill/131029europeaninstituteremarks.pdf y http://www.ftc.gov/speeches/ramirez/131029tacdremarks.pdf

40 Carta de la presidenta de la Comisión Federal de Comercio, Edith Ramirez, a la vicepresidenta Viviane Reding.

41 Carta de la presidenta de la Comisión Federal de Comercio, Edith Ramirez, a la vicepresidenta Viviane Reding.

42 *U.S.-EU Cooperation to Implement the Safe Harbor Framework*, 12 de noviembre de 2013.

5.2. Panel de la UE para la protección de datos

El Panel de la UE para la protección de datos es un órgano creado en virtud de la Decisión de puerto seguro. Está facultado para investigar las quejas presentadas por los particulares relativas a la recogida de datos personales en el contexto de una relación laboral, así como los casos relativos a entidades certificadas que han elegido esta opción para la resolución de litigios con arreglo al marco de puerto seguro (un 53 % de todas las entidades). Está compuesto por representantes de varias autoridades de protección de datos de la UE.

Hasta la fecha ha recibido cuatro quejas (dos en 2010 y dos en 2013); en 2010 remitió dos de ellas a las autoridades nacionales de protección de datos (Reino Unido y Suiza) y está examinando las otras dos. El bajo número de quejas puede explicarse porque, como ya se ha mencionado, sus facultades se limitan fundamentalmente a determinados tipos de datos.

Otro factor que puede explicar en parte el número limitado de quejas es que la existencia del Panel es poco conocida, razón por la cual desde 2004 la Comisión le ha dado más visibilidad en su sitio *web*[43].

A fin de hacer un mejor uso del Panel, las entidades de Estados Unidos que hayan optado por cooperar con él y cumplir sus decisiones, para todas o para parte de las categorías de datos personales cubiertas por sus autocertificaciones respectivas, deberán indicarlo de forma clara y visible en los compromisos asumidos respecto a sus políticas de protección de datos, a fin de que el Departamento de Comercio pueda controlar este aspecto. Los sitios *web* de todas las autoridades de protección de datos de la UE deberían crear una página dedicada al puerto seguro a fin de darlo a conocer mejor a las entidades, y los titulares de datos, europeos.

5.3. Mejora de la aplicación

Los problemas de transparencia y aplicación ya mencionados suscitan inquietud entre las entidades europeas respecto a las repercusiones negativas del marco de puerto seguro sobre su competitividad. Cuando una entidad europea compite con otra estadounidense que está adherida al marco de puerto seguro pero que, en la práctica, no cumple sus principios, la entidad europea se encuentra en una situación de desventaja competitiva.

Es más, la jurisdicción de la Comisión Federal de Comercio se extiende a los actos o prácticas desleales o fraudulentos «en el comercio o en relación con él». El artículo 5 de la *Federal Trade Commission Act* establece una serie de excepciones a dicha jurisdicción que afectan, entre otras, a las **telecomunicaciones.** Al no ser competencia de la Comisión Federal de Comercio, las empresas de telecomunicaciones no pueden adherirse a los principios de puerto seguro. Ahora bien, debido a la creciente convergencia de las tecnologías y los servicios, muchos de sus competidores directos en el sector estadounidense de las tecnologías de la información y la comunicación sí son miembros de puerto seguro. La exclusión de las empresas de telecomunicación de los intercambios de datos con arreglo al marco de puerto seguro preocupa a algunos operadores europeos de telecomunicaciones. Según la Asociación de Operadores Públicos Europeos de Telecomunicación (ETNO en sus siglas en inglés) «ello entra en claro conflicto con la importante reivindicación de los operadores de

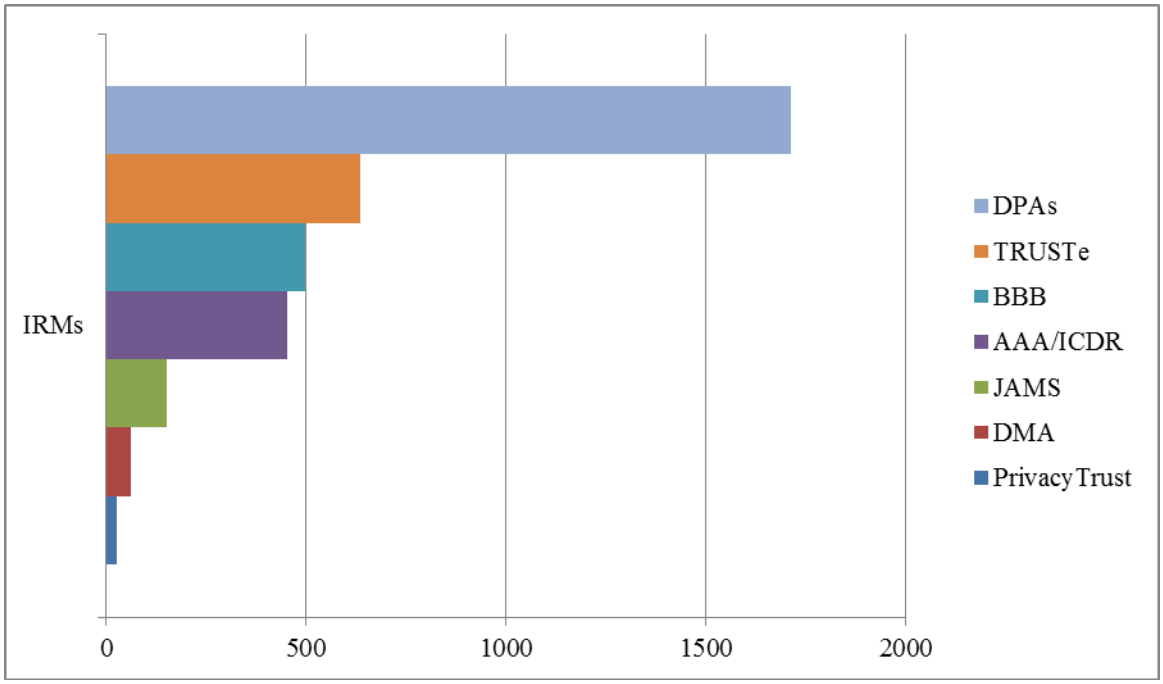
[43] Con arreglo al Informe de 2004, en el sitio *web* de la Comisión (DG Justicia) se ha publicado una nota informativa, en forma de preguntas y respuestas, sobre el Panel de la UE para la protección de datos, con el fin de darlo a conocer a los particulares y ayudarles a presentar una queja si consideran que sus datos personales han sido tratados infringiendo la Decisión de puerto seguro: http://ec.europa.eu/justice/policies/privacy/docs/adequacy/information_safe_harbour_es.pdf.
El formulario para presentar una queja se encuentra en http://ec.europa.eu/justice/policies/privacy/docs/adequacy/complaint_form_en.pdf .

telecomunicación respecto a la necesidad de contar con unas condiciones de competencia equitativas»[44].

6. REFUERZO DE LOS PRINCIPIOS DE PUERTO SEGURO

6.1. Resolución extrajudicial de litigios

El principio de aplicación exige la existencia de «una **vía de recurso independiente, asequible e inmediatamente disponible** para investigar y resolver con arreglo a los principios las quejas y litigios de los particulares». Con este fin, el marco de puerto seguro establece un sistema de solución extrajudicial de litigios por una tercera parte independiente[45] que ofrezca soluciones rápidas a los particulares. Los tres principales mecanismos de recurso son el Panel de protección de datos de la UE, BBB (*Better Business Bureaus*) y TRUSTe.



El recurso a la solución extrajudicial de litigios ha aumentado desde 2004 y el Departamento de Comercio está controlando más a los proveedores estadounidenses de estos servicios con el fin de garantizar que ofrecen información clara, accesible y comprensible sobre el procedimiento de presentación de quejas. No obstante, la efectividad de este sistema todavía está por demostrar, ya que hasta ahora solo se ha tratado un número limitado de casos[46].

---

44 Las observaciones de ETNO, recibidas por los servicios de la Comisión el 4 de octubre de 2013, analizan también 1) la definición de datos personales en puerto seguro, 2) la falta de supervisión del sistema de puerto seguro y 3) el hecho de que «las empresas estadounidenses pueden transferir datos con muchas menos restricciones que sus homólogas europeas», lo que «constituye una discriminación evidente contra las empresas europeas y está afectando a su competitividad». Con arreglo a las normas de puerto seguro, para revelar información a terceros, las entidades deben aplicar los principios de «Notificación» y «Opción». Cuando una entidad desea transmitir información a un tercero que actúe como agente, puede hacerlo si previamente se asegura de que este subscribe los principios, si es objeto de una resolución sobre su adecuación con arreglo a la Directiva u a otra disposición o si firma con él un convenio por escrito para que ofrezca como mínimo el mismo nivel de respeto de la vida privada que el requerido por dichos principios.

45 La Directiva 2013/11/UE relativa a la resolución alternativa de litigios en materia de consumo subraya la importancia de unos procedimientos de resolución alternativa de litigios independientes, imparciales, transparentes, efectivos, rápidos y justos.

46 Por ejemplo, uno de los mayores proveedores de servicios (TRUSTe) comunicó que en 2010 había recibido 881 peticiones, pero que solo tres se consideraron admisibles y fundadas y tuvieron como consecuencia que se obligase a la entidad en cuestión a modificar su política de protección de la vida privada. Según el Departamento de Comercio, la gran mayoría de las quejas que

Aunque el Departamento de Comercio ha conseguido reducir las tarifas de los servicios de solución extrajudicial, dos de los siete proveedores más importantes siguen cobrando a los particulares por presentar una queja[47], lo que significa que en torno al 20 % de las entidades participantes en puerto seguro han seleccionado un proveedor que cobra a los consumidores por presentar quejas. Tales prácticas no cumplen el principio de «Aplicación» de puerto seguro, que confiere a los particulares el derecho a acceder a «una vía de recurso independiente, asequible e inmediatamente disponible». En la Unión Europea, el acceso a un servicio independiente de solución de litigios que facilita el Panel de protección de datos es gratuito para todos los titulares de datos.

El 12 de noviembre de 2013 el Departamento de Comercio confirmó que continuaría defendiendo la vida privada de los ciudadanos de la UE y trabajando con los proveedores de servicios de solución extrajudicial para intentar seguir reduciendo sus tarifas.

En cuanto a las sanciones, no todos los proveedores de estos servicios disponen de las herramientas necesarias para poner remedio a las situaciones de incumplimiento de los principios de protección de la vida privada. Es más, entre la gama de sanciones y medidas que aplican no siempre está previsto hacer públicos los casos de incumplimiento constatados.

Asimismo, los proveedores de servicios de solución extrajudicial deben remitir a la Comisión Federal de Comercio aquellos casos en los que una entidad no cumple el resultado del proceso de solución extrajudicial o rechaza la decisión del proveedor, a fin de que la Comisión Federal pueda llevar a cabo una investigación y, si procede, adoptar medidas de ejecución. Sin embargo, hasta la fecha no se ha producido ningún caso de remisión por parte de los proveedores de estos servicios a la Comisión Federal por incumplimiento[48].

Los proveedores de servicios de solución extrajudicial presentan en sus sitios web listas de las entidades (participantes en la solución de litigios) que utilizan sus servicios. Ello permite a los consumidores comprobar si, en caso de litigio con una entidad, un particular puede presentar una queja a un proveedor de servicios de soluciones extrajudiciales concreto. Así, por ejemplo, el proveedor BBB presenta una lista de todas las empresas acogidas a su sistema de resolución de conflictos. Sin embargo, son muchas las empresas que afirman estar acogidas a un sistema concreto de solución de litigios sin estar incluidas en las listas del proveedor[49].

Los mecanismos de solución extrajudicial de litigios deben ser de fácil acceso, independientes y asequibles para los particulares. Un titular de datos debe poder presentar una queja sin problemas. Todas las instancias de resolución de conflictos deben publicar en sus sitios *web* estadísticas sobre las quejas tramitadas e información sobre su resultado. Por último, estas instancias deben controlarse más para garantizar que la información que facilitan sobre el

---

piden una solución extrajudicial proceden de consumidores, por ejemplo, usuarios que olvidan su contraseña y no pueden obtenerla a través del servicio de internet. A petición de la Comisión Europea, el Departamento de Comercio ha elaborado nuevos criterios para la presentación de estadísticas que deben utilizar todos los proveedores de soluciones extrajudiciales de litigios. Estos criterios distinguen entre simples consultas y quejas, y ofrecen más aclaraciones sobre los tipos de quejas recibidas. No obstante, hay que analizarlos más para garantizar que las nuevas estadísticas de 2014 se refieran a todos los proveedores de soluciones extrajudiciales, sean comparables y ofrezcan información fundamental para valorar la efectividad del mecanismo de recurso.

47 El *International Centre for Dispute Resolution / American Arbitration Association* (ICDR/AAA) cobra una tasa de tramitación de 200 USD y JAMS de 250 USD. El Departamento de Comercio informó a la Comisión que había trabajado con la AAA, el proveedor de estos servicios para particulares más caro, en el desarrollo de un programa específico para puerto seguro que reducía el coste para los consumidores desde varios miles de dólares a una tarifa plana de 200 USD.

48 Véase la pregunta más frecuente número 11.

49 Por ejemplo, Amazon ha comunicado al Departamento de Comercio que recurre a BBB como proveedor de servicios de solución extrajudicial, pero BBB no incluye a Amazon en su lista de participantes. A la inversa, Arsalon Technologies (www.arsalon.net), un proveedor de servicios de alojamiento en nube, aparece en la lista de solución de litigios de puerto seguro de BBB, pero dicha empresa no es actualmente miembro de puerto seguro (a 1 de octubre de 2013). BBB, TRUSTe y otros proveedores de soluciones extrajudiciales deben retirar o corregir las afirmaciones de certificación. Deberían estar vinculados por una obligación exigible de certificar únicamente a las entidades adheridas a puerto seguro.

procedimiento y la forma de presentar una queja es clara y comprensible, de tal modo que la resolución de litigios se convierta en un mecanismo efectivo y fiable que ofrezca resultados. Hay que reiterar también que entre las sanciones obligatorias en la solución extrajudicial de litigios debe incluirse la publicación de la constatación de incumplimiento.

6.2. Transferencia ulterior

El crecimiento exponencial de los flujos de datos hace necesario garantizar la protección permanente de los datos personales en todas las fases de su tratamiento, especialmente cuando son transferidos desde una empresa adherida a puerto seguro a **un tercero encargado de su tratamiento**. Por tanto, la necesidad de respetar el marco de puerto seguro no solo afecta a sus miembros, también a los subcontratistas.

El marco de puerto seguro permite la transferencia ulterior a un tercero que actúe como «agente» si previamente la empresa - adherida a puerto seguro - «se asegura de que este subscribe los principios, si es objeto de una resolución sobre su "adecuación" con arreglo a la Directiva u otra disposición o si firma con él un convenio por escrito para que ofrezca como mínimo el mismo nivel de protección de la vida privada que el requerido por dichos principios»[50]. Por ejemplo, un proveedor de servicios en nube es invitado por el Departamento de Comercio a suscribir un contrato, incluso aunque cumpla los principios de puerto seguro y reciba datos personales para su tratamiento[51]. No obstante, esta disposición no queda clara en el anexo II de la Decisión de puerto seguro.

Puesto que el recurso a subcontratistas ha aumentado considerablemente en los últimos años, especialmente en el contexto de la computación en nube, al suscribir un contrato de este tipo una entidad miembro de puerto seguro debe notificarlo al Departamento de Comercio y está obligada a hacer públicas las garantías de protección de la intimidad[52].

Las tres cuestiones mencionadas: el mecanismo para la solución extrajudicial de litigios, el refuerzo de la supervisión y las transferencias ulteriores de datos, requieren más aclaraciones.

7. ACCESO A LOS DATOS TRANSFERIDOS EN EL MARCO DE PUERTO SEGURO

A lo largo de 2013 la información sobre la escala y el alcance de los programas estadounidenses de vigilancia han suscitado inquietudes sobre la continuidad de la protección de los datos personales transferidos a Estados Unidos con arreglo al marco de puerto seguro. Por ejemplo, aparentemente todas las empresas involucradas en el programa PRISM, y que conceden a las autoridades estadounidenses acceso a los datos almacenados y tratados en Estados Unidos, tienen el certificado de puerto seguro. Esto ha hecho de puerto seguro uno de los conductos a través de los cuales se da acceso a las autoridades de inteligencia estadounidenses para recopilar datos personales que han sido tratados inicialmente en la UE.

La Decisión de puerto seguro establece en su anexo I que la adhesión a los principios de protección de la vida privada puede limitarse si así lo justifican las exigencias de seguridad

50 Véase la Decisión de la Comisión 2000/520/CE, página 8 (transferencia ulterior).

51 Véase: *Clarifications Regarding the U.S.-EU Safe Harbor Framework and Cloud Computing*: http://export.gov/static/Safe%20Harbor%20and%20Cloud%20Computing%20Clarification_April%2012%202013_Latest_eg_main_060351.pdf

52 Estas observaciones se refieren a los proveedores de servicios en nube que no están adheridos a puerto seguro. Según la consultoría Galexia, «el nivel de adhesión (y cumplimiento) entre los proveedores de servicios en nube es bastante elevado. Normalmente los proveedores de estos servicios disponen de múltiples capas de protección de la intimidad, combinando muchas veces contratos directos con clientes y políticas generales de protección de la intimidad. Con una o dos excepciones importantes, los proveedores de servicios en nube en el marco de puerto seguro cumplen las principales disposiciones en materia de solución de litigios y aplicación. En este momento no hay ningún proveedor importante de servicios en nube en la lista de alegaciones falsas de adhesión». (Comparecencia de Chris Connolly, de Galexia, en la investigación de la Comisión LIBE sobre la vigilancia electrónica a gran escala de ciudadanos de la UE).

nacional, interés público y cumplimiento de la ley, o por disposición legal o reglamentaria o jurisprudencia. Para ser válidas, las limitaciones y restricciones al disfrute de los derechos fundamentales deben interpretarse restrictivamente, deben presentarse en una legislación accesible al público y deben ser necesarias y proporcionadas en una sociedad democrática. En particular, la Decisión de puerto seguro especifica que tales limitaciones se permiten únicamente **«cuanto sea necesario»** para cumplir las exigencias de seguridad nacional, interés público y cumplimiento de la ley[53]. Si bien el marco de puerto seguro prevé excepcionalmente el tratamiento de datos con fines de seguridad nacional, interés público o cumplimiento de la ley, en el momento de su adopción no era previsible el acceso a gran escala de las agencias de inteligencia a los datos transferidos a Estados Unidos en el contexto de transacciones comerciales.

Es más, por razones de transparencia y seguridad jurídica el Departamento de Comercio debe comunicar a la Comisión Europea cualquier disposición legal o reglamentaria que pudiera afectar a la adhesión a los principios de puerto seguro para la protección de la vida privada[54]. Hay que controlar cuidadosamente el recurso a excepciones, y dichas excepciones no se utilizarán de forma tal que socaven la protección ofrecida por los **principios**[55]. En particular, el acceso a gran escala por parte de las autoridades estadounidenses a los datos tratados por entidades con autocertificación de puerto seguro corre el peligro de socavar la confidencialidad de las comunicaciones electrónicas.

7.1. Proporcionalidad y necesidad

Como se desprende de las conclusiones del Grupo de trabajo *ad hoc* UE-EE.UU. sobre protección de datos, diversas bases legales con arreglo al ordenamiento jurídico estadounidense permiten la recogida y el tratamiento a gran escala de datos personales almacenados o tratados de otra forma por entidades basadas en Estados Unidos. Ello puede incluir los datos transferidos previamente desde la UE a EE.UU. con arreglo al marco de puerto seguro, y plantea la cuestión de si se siguen respetando sus principios. Al tratarse de programas a gran escala, puede ocurrir que las autoridades estadounidenses accedan y procesen los datos transferidos al amparo del puerto seguro más allá de lo estrictamente necesario y proporcionado para la protección de la seguridad nacional, como reza la excepción prevista en la Decisión de puerto seguro.

7.2. Limitaciones y posibilidades de reparación

Como se desprende de las constataciones del Grupo de trabajo *ad hoc* UE-EEUU sobre protección de datos, las garantías previstas por la legislación estadounidense se refieren fundamentalmente a los ciudadanos estadounidenses o a los residentes legales. Es más, no está prevista la posibilidad de que los titulares de los datos, ya sean estadounidenses o de la UE, puedan acceder a sus datos, rectificarlos o suprimirlos, ni obtener reparación

53 Véase el anexo 1 de la Decisión de puerto seguro: « La adhesión a estos principios puede limitarse: a) cuanto sea necesario para cumplir las exigencias de seguridad nacional, interés público y cumplimiento de la ley; b) por disposición legal o reglamentaria, o jurisprudencia que originen conflictos de obligaciones o autorizaciones explícitas, siempre que las entidades que recurran a tales autorizaciones puedan demostrar que el incumplimiento de los principios se limita a las medidas necesarias para garantizar los intereses legítimos esenciales contemplados por las mencionadas autorizaciones; 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 Estados Unidos de América, se espera que las entidades opten por el mayor nivel de protección posible».

54 Dictamen 4/2000 sobre el nivel de protección ofrecido por los principios de puerto seguro, adoptada por el Grupo de trabajo sobre protección de datos del artículo 29 el 16 de mayo de 2000.

55 Ídem.

administrativa o judicial, en lo que respecta a la recogida y el tratamiento posterior de sus datos personales en virtud de los programas de vigilancia estadounidenses.

7.3. Transparencia

Las entidades no indican sistemáticamente en sus políticas de protección de la vida privada cuándo aplican excepciones a los principios. Así, los particulares y las entidades no saben qué se está haciendo con sus datos, lo que reviste especial importancia en relación con los programas de vigilancia estadounidenses en cuestión. En consecuencia, los europeos cuyos datos se han transferido a entidades en Estados Unidos con arreglo al marco de puerto seguro pueden no ser conscientes, ya que tales entidades no se lo comunican, de que es posible que se acceda a sus datos[56]. Esto plantea la cuestión del cumplimiento de los principios de puerto seguro en lo que respecta a la transparencia. Es necesario garantizar la transparencia en la mayor medida posible sin poner en peligro la seguridad nacional. Además de exigir a las entidades que indiquen en sus políticas de protección de la vida privada en qué circunstancias la adhesión a los principios de puerto seguro puede verse limitada por disposición legal o reglamentaria, o por jurisprudencia, conviene animarlas a explicar en sus políticas de protección de la vida privada en qué casos aplican excepciones a los principios para satisfacer exigencias de seguridad nacional, interés público o cumplimiento de la ley.

8. CONCLUSIONES Y RECOMENDACIONES

Desde su adopción en 2000, el marco de puerto seguro se ha convertido en un vehículo para los flujos de datos personales entre la UE y EE.UU. La importancia de una protección eficaz cuando se transfieren datos personales es cada vez mayor, debido al aumento exponencial de los flujos de datos, fundamental para la economía digital, y a los notables avances en materia de recogida, tratamiento y utilización de los datos. Las empresas de la red, como Google, Facebook, Microsoft, Apple o Yahoo, tienen centenares de millones de clientes en Europa y transfieren datos personales para su tratamiento en Estados Unidos a una escala inconcebible en el año 2000, cuando se creó el marco de puerto seguro.

Las deficiencias en lo que respecta a la transparencia y la aplicación del marco hacen que persistan problemas concretos que deben solucionarse:

a) la transparencia de las políticas de protección de la vida privada de los miembros de puerto seguro;

b) la aplicación efectiva de los principios de protección de la vida privada por parte de las entidades en Estados Unidos; y

c) el carácter efectivo de la aplicación.

Por otra parte, el **acceso a gran escala por parte de las agencias de inteligencia a los datos transferidos a Estados Unidos por entidades con certificación de puerto seguro** suscita serias cuestiones adicionales en lo que respecta al derecho de los europeos a que sus datos sigan estando protegidos cuando se transfieren a ese país.

Partiendo de todo lo expuesto, la Comisión ha elaborado las **recomendaciones** siguientes:

[56] Algunas entidades europeas adheridas a puerto seguro facilitan información relativamente transparente a este respecto. Por ejemplo, Nokia, que opera en Estados Unidos y es miembro de puerto seguro, facilita la siguiente información en su política de privacidad: «Las leyes vigentes nos pueden obligar a revelar tus datos personales a ciertas autoridades y otros terceros, como por ejemplo, a los cuerpos y fuerzas de seguridad del Estado en los países en los que operemos nosotros, o terceros que actúen en nuestro nombre».

Transparencia

1. *Las entidades autocertificadas deberán hacer públicas sus políticas de protección de la vida privada*. No basta con que faciliten al Departamento de Comercio una descripción de sus políticas de protección de la vida privada; deben ponerlas a disposición del público en sus sitios *web*, de forma visible y en un lenguaje claro.

2. *Las políticas de protección de la vida privada que figuren en los sitios* web *de las entidades autocertificadas deberán incluir siempre un vínculo al sitio del Departamento de Comercio dedicado al puerto seguro, que contiene una lista de todos los miembros «actualizados» del sistema*. Ello permitirá a los titulares europeos de los datos comprobar inmediatamente, sin necesidad de más búsquedas, si una entidad está adherida al marco de puerto seguro actualmente. De esta forma se reducirán las posibilidades de alegaciones falsas de adhesión y aumentará la credibilidad del sistema. En mayo de 2013 el Departamento de Comercio comenzó a exigir este requisito a las entidades, pero es necesario intensificar el proceso.

3. *Las entidades autocertificadas deberán hacer públicas las condiciones de respeto de la vida privada de todo contrato que celebren con subcontratistas, como los servicios de computación en nube*. El sistema de puerto seguro permite la transferencia ulterior desde entidades autocertificadas a terceros que actúen como «agentes», por ejemplo, a proveedores de servicios de computación en nube. Entendemos que, en tales casos, el Departamento de Comercio exige a las entidades autocertificadas que suscriban un contrato. No obstante, cuando suscriban este tipo de contrato las entidades deberán notificarlo también al Departamento de Comercio y hacer públicas las garantías de protección de la intimidad.

4. *El sitio* web *del Departamento de Comercio deberá indicar claramente todas las entidades que actualmente no son miembros del sistema.* La etiqueta «No actualizada» (*Not current*) en la lista de miembros de puerto seguro del Departamento de Comercio debería ir acompañada de la advertencia de que dicha entidad no cumple actualmente los requisitos de puerto seguro. A pesar de ello, una entidad cuya certificación figure como «No actualizada» está obligada a seguir aplicando los requisitos de puerto seguro a los datos que haya recibido con arreglo a dicho marco.

Recursos

5. *Las políticas de protección de la vida privada que figuren en los sitios* web *de las entidades deberán incluir un vínculo a su proveedor de servicios de solución extrajudicial de litigios o al Panel de la UE.* Ello permitirá a los titulares europeos de los datos ponerse en contacto inmediatamente con el proveedor o con el Panel de la UE en caso de problema. En marzo de 2013 el Departamento de Comercio comenzó a exigir este requisito a las entidades, aunque el proceso debería intensificarse.

6. *Los servicios de solución extrajudicial de litigios deberán ser asequibles y estar fácilmente disponibles*. Algunos proveedores de servicios de solución extrajudicial en el marco de puerto seguro siguen cobrando por tramitar las quejas (200-250 USD), lo que puede resultar muy caro para los particulares. En Europa, en cambio, el acceso al Panel de protección de datos previsto para la solución de litigios en el marco de puerto seguro es gratuito.

7. *El Departamento de Comercio debe supervisar de manera más sistemática a los proveedores de servicios de solución extrajudicial de litigios en lo que respecta a la*

transparencia y la accesibilidad de la información que facilitan sobre sus procedimientos y sobre el seguimiento dado a las quejas. De esta forma la solución de litigios se convertirá en un mecanismo efectivo y fiable que ofrece resultados. Conviene reiterar que entre las sanciones obligatorias impuestas por los organismos de solución extrajudicial debe incluirse la publicación de las constataciones de incumplimiento.

Aplicación

8. *Tras la certificación o la renovación de la certificación de las entidades, conviene someter a un porcentaje de ellas a investigaciones de oficio para comprobar el cumplimiento efectivo de sus políticas de protección de la vida privada (yendo más allá del mero control del cumplimiento de las exigencias formales).*

9. *Siempre que se constate un incumplimiento a raíz de una queja o una investigación, deberá someterse a la entidad a una investigación específica al cabo de un año.*

10. *Cuando existan dudas sobre el cumplimiento por parte de una entidad, o si hay quejas pendientes, el Departamento de Comercio deberá comunicarlo a la autoridad de protección de datos de la UE competente.*

11. *Hay que seguir investigando las afirmaciones falsas de adhesión a puerto seguro.* Una entidad que afirme en su sitio *web* que cumple los requisitos de puerto seguro pero que no figure en la lista del Departamento de Comercio como miembro con certificación «actualizada» (*current*) está engañando a los consumidores y abusando de su confianza. Las afirmaciones falsas debilitan la credibilidad del marco en su conjunto, por lo que deben ser retiradas inmediatamente de los sitios *web* de las entidades.

Acceso por parte de las autoridades estadounidenses

12. *Las políticas de protección de la vida privada de las entidades autocertificadas deben incluir información sobre la medida en que la legislación estadounidense permite a las autoridades públicas recoger y tratar datos transferidos al amparo de puerto seguro. En particular, hay que animar a las entidades a indicar en sus políticas de protección de la vida privada en qué circunstancias aplican excepciones a los principios con el fin de cumplir exigencias de seguridad nacional, interés público o cumplimiento de la ley.*

13. *Es importante que la excepción relativa a la seguridad nacional prevista en la Decisión de puerto seguro no se utilice más allá de lo estrictamente necesario o proporcionado.*