El nuevo acuerdo entre la Unión Europea y Estados Unidos para la transferencia de datos personales compartidos en redes sociales

New EU-US agreement about transfers of data shared in social networks

Alicia Chicharro – Universidad Pública de Navarra –
alicia.chicharro@unavarra.es

Abstract: El respeto a la vida privada como derecho fundamental auspicia las normas europeas sobre protección de datos personales. Esas normas permiten la transferencia de este tipo de datos a terceros países fuera de la UE siempre que los mismos garanticen un nivel de protección adecuado.

Con respecto a las transmisiones entre empresas privadas -entre ellas las proveedoras de las más famosas redes sociales-, la sentencia del Tribunal de Justicia en el caso Facebook invalidó la decisión adoptada por la Comisión en la que, apoyándose en el régimen de puerto seguro, consideraba que la legislación estadounidense garantizaba un nivel adecuado de protección de los datos personales transferidos desde la Unión a entidades establecidas en Estados Unidos.

A partir de ese momento la Comisión decidió iniciar un proceso de negociación con las autoridades estadounidenses para diseñar un nuevo sistema, denominado “escudo de privacidad”, que culminó en el acuerdo alcanzado por la UE y EEUU en julio de 2016.

En la presente comunicación analizaremos este nuevo régimen de transferencia de datos de ciudadanos europeos a empresas americanas como Facebook, Google, Dropbox o Yahoo, tomando en consideración las mejoras

respecto al sistema de puerto seguro, a la vez que se señalarán las deficiencias que aún presenta y que pueden poner en riesgo la privacidad de millones de usuarios en toda Europa.

Keywords: Datos personales; privacidad; redes sociales; acuerdos UE-EEUU

1. Introducción

La protección de datos de carácter personal es un derecho fundamental de vital importancia en la era digital. El artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea así lo proclama y añade que los "datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley".

La transferencia masiva de datos de carácter personal de ciudadanos europeos tanto a las autoridades públicas, como a las empresas privadas de Estados Unidos siempre ha estado rodeada de polémica. Garantizar el flujo de datos desde la Unión a cualquier país tercero requiere que la normativa de ese país ofrezca protección jurídica contra posibles arbitrariedades e indique claramente el alcance de la discrecionalidad y de las potestades de las autoridades públicas. La defensa del derecho a la intimidad y a la privacidad desarrollada por la legislación europea y adoptada internamente en cada uno de los Estados miembros se esgrime como paradigma de aptitud para la protección de los datos personales de los ciudadanos europeos no sólo en la Unión, sino también en las transferencias de los mismos a terceros países.

Revelaciones de tratamiento masivo de esos datos como las que formuló Edward Snowden[1], llevan a preguntarse si aquello que protegemos tan celosamente con nuestra normativa europea a nivel interno de la Unión, se ve despojado de la mayor parte de sus garantías cuando se transmite a las empresas o autoridades estadounidenses.

[1] A través del programa PRISM, la Agencia de Seguridad Nacional de Estados Unidos (NSA) vigilaba electrónicamente a los usuarios europeos de compañías como Facebook, Google, Yahoo, Dropbox, Apple o Microsoft. Los datos que supuestamente la NSA es capaz de obtener gracias a PRISM incluyen correos electrónicos, videos, chat de voz, fotos, direcciones IP, notificaciones de inicio y fin de sesión, transferencia de archivos y detalles de perfiles de las redes sociales.

La piedra angular de la normativa sobre protección de datos en la UE es la Directiva 95/46/CE[2]. Esta Directiva dispone que en principio solo se pueden transferir dichos datos a un país tercero si éste garantiza un nivel de protección adecuado (Kuner, 2013: 65). Así, la Comisión puede declarar que un Estado fuera de la Unión asegura de una forma correcta los datos personales atendiendo a sus normas internas o a los instrumentos internacionales para los que ha prestado su consentimiento en obligarse.

La Comisión Europea y el Departamento de Comercio de los Estados Unidos habían negociado un acuerdo por el que se establecía un régimen de autocertificación, al que las empresas se adherían voluntariamente, denominado programa o régimen de "puerto seguro"[3]. En base a los principios contenidos en el mismo, la Comisión dictó la Decisión 2000/520/CE[4], afirmando que las transferencias de datos personales desde la Unión a Estados Unidos cumplían las salvaguardas contenidas en la Directiva 95/46/CE, por tanto, su nivel de protección se consideraba adecuado.

Sin embargo, el 6 de octubre de 2015, el Tribunal de Justicia de la Unión Europea (TJUE) dictó una trascendente sentencia en la que declaró inválida dicha Decisión[5]. La petición de dictamen perjudicial tenía por objeto la interpretación de los artículos 7, 8 y 47 de la Carta de los Derechos Fundamentales de la Unión Europea, así como los artículos 25.6 y 28 de la Directiva sobre protección de datos.

[2] 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, (DO L 281, página 31), modificada por el Reglamento (CE) 1882/2003 (DO L 284, página 1).

[3] US-EU Safe Harbor Overview, recuperado el 15 de octubre de 2015 de http:export.gov/ safeharbor/eu/eg_main_018476.asp. El régimen de puerto seguro incluye una serie de principios relativos a la protección de datos personales a los que las empresas estadounidenses pueden suscribirse voluntariamente. Tanto los principios como las preguntas más frecuentes (FAQ), en las que se proporciona orientación para aplicar los principios, fueron publicados por el Gobierno de Estados Unidos con fecha 21 de julio de 2000 y aparecen como anexos de la Decisión 2000/520/CE.

[4] Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE, 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 L 215, página 7).

[5] STJUE, 6 de octubre de 2015, Maximillian Schrems y Data Protection Commissioner, C-362/14, EU:C:2015:650.

La UE y Estados Unidos mantienen fuertes lazos comerciales. Las transferencias de datos personales constituyen una parte importante y necesaria de la relación transatlántica, en particular, en la economía digital global de hoy (Comisión Europea, 2016: 11). Lo cierto es que los flujos masivos de datos de carácter personal hacia empresas como Facebook, Twitter o Google, cuyas sedes centrales se encuentran en territorio americano, son regulares. Estas transferencias afectan a un gran número de personas, cuyos derechos fundamentales pueden verse vulnerados, pero además a una gran cantidad de datos personales. Tanto la Unión como los Estados miembros tienen la obligación de garantizar a los ciudadanos europeos una protección eficaz de sus datos de carácter personal, incluso en el caso de que los mismos se transmitan a terceros países. Por ello, los posibles abusos que se puedan cometer deben ser oportunamente investigados, comprobados y, en su caso, sancionados, restableciéndose inmediatamente el nivel de protección que garantiza el Derecho de la Unión.

Tras la sentencia del Tribunal de Justicia invalidando la Decisión que acogía el régimen de puerto seguro, la Comisión Europea y el Departamento de Comercio de Estados Unidos han negociado un nuevo programa denominado escudo de privacidad. Gracias a las garantías que este ofrece, la Comisión ha dictado una nueva Decisión por la que considera que la protección de los datos personales que se transfieren a las empresas adheridas al nuevo sistema es la adecuada[6]. A continuación analizaremos ambos regímenes, poniendo de relieve los puntos más problemáticos e indicando si se han conseguido abordar eficazmente a través del acuerdo más reciente.

2. El régimen de puerto seguro

2.1. ¿Un nivel de protección "adecuado"?

Los principios en los que se basaba el régimen de puerto seguro fueron publicados por el Departamento de Comercio de Estados Unidos, junto a una

[6] Decisión de Ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE.UU. (DO L 207, página 1).

serie de preguntas más frecuentes (FAQ) que los complementaban e instruían su aplicación en la práctica[7].

En el artículo 1.1 de su Decisión, la Comisión manifestaba que esos principios, aplicados de conformidad con la orientación que proporcionan las FAQ, garantizaban un nivel adecuado de protección de los datos personales transferidos desde la Unión a entidades establecidas en Estados Unidos (Wolf, 2014: 231).

Cualquier compañía que quería adherirse al régimen de puerto seguro debía desarrollar una política de privacidad sujeta a los principios de notificación, elección, transferencia sucesiva, seguridad, integridad de los datos, acceso y ejecución. No se trataba de normas vinculantes, sino de una serie de directrices voluntarias que una organización podía certificar que seguía (Greer, 2011: 143).

Como la Directiva, los principios incluidos en el régimen de puerto seguro buscaban empoderar al sujeto, exigiendo que fuera informado sobre el fin para el que sus datos iban a ser usados, dándole la oportunidad de elegir si podían ser utilizados para finalidades distintas de las que en un principio justificaron su recogida, y permitiéndole el acceso para corregirlos, enmendarlos o suprimirlos cuando fuera necesario.

Los principios también imponían obligaciones al responsable del tratamiento, como asegurarse de que los datos personales eran relevantes y fiables para el fin pretendido y que solo fueran transferidos a organizaciones consideradas "adecuadas". Además, los responsables del tratamiento debían tomar las precauciones necesarias para proteger los datos personales de posibles pérdidas o abusos y prever un mecanismo de recurso en manos de los particulares para resolver las controversias sobre privacidad y reclamar los posibles daños producidos[8].

[7] Los principios figuran en el anexo I y las FAQ en el anexo II de la Decisión 2000/520/CE. También se pueden consultar todo lo relacionado con el programa de puerto seguro (principios, FAQ, lista de empresas adheridas, políticas de privacidad de dichas empresas, entidades que no han renovado, etc.) en la siguiente página: http:export.gov/safeharbor/eu/eg_main_018476.asp.

[8] El mecanismo de resolución de conflictos podía ser proporcionado a través de órganos autoregulados provenientes del sector privado, entidades legales o reglamentarias de supervisión o comprometiéndose a cooperar con las autoridades europeas de protección de

Cuando una compañía desarrollaba una política de privacidad integral basada en los siete principios del régimen de puerto seguro debía hacerla accesible al público en general, por ejemplo, publicándola en su página web. De otra forma, los individuos cuyos datos personales eran recopilados y sometidos a tratamiento no conocían sus derechos y tampoco eran conscientes de las obligaciones a las que la compañía estaba sometida[9].

Resumiendo, cuando una compañía promulgaba reglas prácticas para el tratamiento de datos personales de acuerdo con los principios, incentivaba el cumplimiento de las mismas a través de una política de privacidad públicamente accesible, establecía un mecanismo independiente de resolución de conflictos que daba respuesta a las posibles reclamaciones y, por último, implementaba un sistema para verificar la futura conformidad con los principios, entonces esa compañía estaba preparada para participar formalmente en el régimen de puerto seguro (Colonna, 2014: 205).

Lo cierto es que la adhesión de una entidad a los principios de puerto seguro se llevaba a cabo conforme a un sistema de autocertificación[10]. Esto significa que la compañía americana señalaba que suscribía los principios y que los cumplía realmente, dentro de su política de privacidad. A continuación notificaba al Departamento de Comercio de Estados Unidos su conformidad con esos principios. Anualmente cada compañía debía renovar su inscripción en dicho registro certificando que seguía cumplimiento con los requisitos de puerto seguro. Si una empresa salía de la lista, las reglas de protección garantizadas por el régimen de puerto seguro se seguirían aplicando a los datos que fueron obtenidos durante el periodo que se acogió a los principios asociados a tal régimen.

---

datos. Un ejemplo de la primera opción lo constituye TRUSTe, una organización de solución de disputas que ya ha tomado decisiones en más de 4.000 reclamaciones presentadas por ciudadanos europeos frente a compañías estadounidenses acogidas al régimen de puerto seguro. En Europa, el Panel de protección de datos de la UE también ofrece solución extrajudicial de los litigios y, al contrario que las entidades americanas, es totalmente gratuito. Solo cuando el mecanismo elegido no es capaz de resolver la controversia, el asunto sería remitido a la agencia gubernamental estadounidense que tenga jurisdicción sobre la compañía en cuestión (normalmente se trata de la Federal Trade Commission).

[9] Comunicación de la Comisión al Parlamento Europeo y al Consejo, de 27 de noviembre de 2013, 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.

[10] Artículo 1, apartados 2 y 3, de la Decisión 2000/520, en relación con la FAQ nº 6, anexo II.

Como decimos el Departamento de Comercio estadounidense era el encargado de recibir y revisar todas las autocertificaciones de adhesión a los principios de puerto seguro y todas las comunicaciones anuales de renovación, manteniendo al día una lista con las empresas que habían presentado esta documentación. Pero para el caso de declaraciones falsas de adhesión o incumplimiento de los principios de puerto seguro por parte de entidades participantes, la encargada de la investigación era la Comisión Federal de Comercio (*Federal Trade Commission*), que interviene contra prácticas desleales y fraudulentas para los consumidores conforme a la *Federal Trade Commission Act* de 1914[11].

2.2. Dudas suscitadas por el programa de puerto seguro

2.2.1. Reticencias oficiales

Sin duda el programa de puerto seguro había conseguido dinamizar los flujos de datos personales transferidos desde la UE a las compañías estadounidenses, de una manera uniforme para todos los Estados miembros, desechando el peligro de acudir de forma extensiva a las excepciones del artículo 26 (Blume, 2000: 78). Sin embargo, este programa ya había sido criticado en la UE, crítica que se intensificó a raíz de las revelaciones realizadas por Edward Snowden en junio de 2013.

Antes de eso, en julio de 2012, el Grupo de Trabajo del Artículo 29 advirtió que los exportadores europeos de datos personales a empresas americanas no deberían fiarse solo de la autocertificación y exigir pruebas de cumplimiento de los principios de puerto seguro[12]. Tras el escándalo de las escuchas ilegales, el Parlamento Europeo solicitó a la Comisión que revisará el régimen de puerto

[11] En el caso específico de la aplicación de los principios de puerto seguro a las compañías aéreas, el órgano competente era el Departamento de Transporte de Estados Unidos (Título 46, § 41712 US Code).

[12] GT29, Dictamen 05/2012 sobre computación en la nube, WT 196, 1 de julio de 2012. Con anterioridad, el Düsseldorfer Kreis, un grupo de trabajo que abarca las 16 autoridades de protección de datos en el sector privado de los Länder alemanes, adoptó una resolución en la que requería más diligencia por parte de los exportadores de datos personales alemanes que transmitieran a entidades acogidas al programa de puerto seguro. Con ello, sin duda, se ponía en tela de juicio que la Decisión 2000/520/CE demostrara suficientemente un nivel adecuado de protección de los datos personales por parte de las empresas estadounidenses adheridas.

seguro, a la vista de que el acuerdo que le servía de base había sido gravemente violado por las autoridades estadounidenses[13].

En sus dos primeros informes sobre la aplicación del programa puerto seguro, publicados en 2002[14] y 2004[15], la Comisión identificó varias deficiencias en lo que respecta a la adecuada aplicación de los principios y realizó diversas recomendaciones a las autoridades estadounidenses para su rectificación.

En su tercer informe de aplicación de 2013, nueve años después del segundo informe y sin que ninguna de las deficiencias reconocidas hubiese sido rectificada, la Comisión identificó otros defectos de amplio alcance en el régimen de puerto seguro y concluyó que no podía mantenerse la aplicación actual[16]. Tengamos en cuenta además que en ese momento ya se habían producido las revelaciones de Snowden.

La Comisión dirigió 13 recomendaciones a las autoridades estadounidenses y se comprometió a identificar para el verano de 2014, junto con dichas autoridades, un paquete de medidas correctivas que habían de aplicarse lo antes posible, creando la base para una revisión total del funcionamiento de los principios de puerto seguro.

Las autoridades de control de algunos Estados miembros también habían criticado la formulación excesivamente general de los principios, así como la

[13] Resolución del Parlamento Europeo, de 12 de marzo de 2014, sobre el programa de vigilancia de la Agencia Nacional de Seguridad de los EEUU, los órganos de vigilancia en diversos Estados miembros y su impacto en los derechos fundamentales de los ciudadanos de la UE y en la cooperación trasatlántica en materia de justicia y asuntos de interior. Con anterioridad, en su Resolución de 5 de julio de 2000 sobre sobre el proyecto de Decisión de la Comisión relativa a la adecuación de la protección conferida por los principios de puerto seguro y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América, el Parlamente Europeo expresó sus dudas e inquietudes acerca de la adecuación de los principios de puerto seguro y pidió a la Comisión que revisara la decisión con prontitud, a la luz de la experiencia y de los desarrollos legislativos. La Comisión volvió a examinar el proyecto de Decisión a la luz de dicha Resolución y llegó a la conclusión de que, a pesar de la opinión expresada por el Parlamento Europeo, aquél no declara en ningún momento que al adoptar la Decisión vaya más allá de sus competencias.

[14] The application of Commission Decision 520/2000/CE of 26 July 2000 pursuant the 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, 13 December 2002.

[15] The implementation of Commission Decision 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, 20 October 2004.

[16] Comunicación de la Comisión al Parlamento Europeo y al Consejo, de 27 de noviembre de 2013, 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.

dependencia de la autocertificación y la autorregulación[17]. En ningún momento se mencionaba si se habían llevado a cabo las constataciones suficientes sobre las medidas con las que Estados Unidos garantizaba un nivel de protección adecuado. Sin embargo, pese a las quejas recibidas ninguna de esas autoridades decidió suspender los flujos de datos a las empresas estadounidenses.

Lo cierto es que el recurso por parte de un país tercero a un sistema de autocertificación no es por sí mismo contrario a lo dispuesto en el artículo 25.6 de la Directiva 95/46/CE. La fiabilidad de este sistema en relación con la exigencia de un nivel de protección adecuado descansa, en esencia, en el establecimiento de mecanismos eficaces de detección y control que permitan identificar y sancionar en la práctica las posibles infracciones de las reglas que garantizan la protección de los derechos fundamentales, en especial del derecho al respeto de la vida privada y del derecho a la protección de los datos personales.

2.2.2. Desconfianza del sector privado

Por su parte, la industria europea expresó su queja debido a la laxitud del sistema que conllevaba distorsiones de la competencia, ya que las empresas americanas se acomodaban a un marco de adhesión voluntaria, autocertificación y autorregulación, muy lejos de las exigencias en materia de protección de datos a las que se ven sometidas las compañías europeas.

Igualmente el hecho de que las empresas estadounidenses pudieran transferir datos con muchas menos restricciones que sus homólogas europeas afectaba a la competitividad de estas últimas. Además, cuando una entidad europea competía con otra americana que estaba adherida al marco de puerto seguro pero que, en la práctica, no cumplía sus principios, la primera se encontraba en situación de desventaja competitiva. A ello había que sumar que las empresas europeas exportadoras de datos a compañías estadounidenses, esto es, las que utilizaban el sistema, también sufrían los efectos adversos al revertirse la

[17] Concretamente las autoridades de control de datos de los Länder alemanes en 2010 y en 2013, la de Irlanda y la de Luxemburgo en 2013.

responsabilidad por las prácticas desleales o fraudulentas de las americanas que los importaban.

Resultaba además que los principios de puerto seguro eran de utilización exclusiva de las entidades privadas estadounidenses que recibían datos de carácter personal de la UE[18]. Por tanto, no se exigía cumplir con dichos principios a las autoridades públicas de Estados Unidos.

2.2.3. Dudas ante la intervención de agencias públicas

No solo existía una falta de imposición de los principios de puerto seguro a las agencias estatales estadounidenses, sino que la Decisión 2000/520/CE tampoco indicaba las normas que en ese país limitarían las posibles injerencias por parte de los poderes estatales en los derechos fundamentales de las personas cuyos datos se transfirieran desde la Unión a dicho Estado, cuando se perseguían fines legítimos como la seguridad nacional.

Si conforme a la propia Decisión, la aplicabilidad de los principios de puerto seguro se podía limitar, en especial, por "las exigencias de seguridad nacional, interés público y cumplimiento de la ley", así como por "disposición legal o reglamentaria, o jurisprudencia, que originen conflictos de obligaciones o autorizaciones"[19], se estaba reconociendo la primacía de esas exigencias sobre los principios. Un reconocimiento que no vino sostenido por una aclaración del ámbito de aplicación de dicha excepción, a fin de evitar cualquier interpretación o aplicación que anulase en esencia el derecho fundamental a la protección de datos. Dicha primacía conllevaba que las entidades americanas autocertificadas que recibieran datos personales desde la Unión estaban obligadas sin limitación a dejar de lado los principios cuando éstos entraran en

[18] Los mecanismos de arbitraje privado y los procedimientos ante la Comisión Federal de Comercio, cuyas facultades estaban descritas en la FAQ nº 11, se limitaban a los litigios comerciales, atañían al cumplimiento por la empresas estadounidenses de los principios de puerto seguro y no se podían aplicar a los litigios concernientes a la legalidad de injerencias en los derechos fundamentales derivadas de medidas de origen estatal. Véanse los puntos 204 a 206 de las conclusiones del Abogado General en el asunto C-362/14.

[19] Anexo I, párrafo cuarto, de la Decisión 2000/520/CE. En este sentido, en el título B del anexo IV se ponía de relieve, respecto a los límites a los que estaba sometida la aplicabilidad de los principios de puerto seguro, que "es evidente que, si la legislación estadounidense establece una obligación en contrario, las entidades deben cumplirla, dentro o fuera del ámbito de puerto seguro".

conflicto con las exigencias mencionadas y su aplicación se manifestase incompatible con ellas.

Esta excepción dejaba la puerta abierta a posibles injerencias en nombre de la seguridad nacional, el interés público o el cumplimiento de la ley estadounidense, en los derechos fundamentales de las personas cuyos datos personales se transfiriesen o pudieran ser transferidos desde la Unión a Estados Unidos.

En este sentido, para demostrar la existencia de una injerencia en la vida privada de una persona carecía de relevancia que la información de que se tratase tuviera o no carácter sensible o que los interesados hubiesen sufrido o no inconvenientes en razón de tal injerencia[20].

En todo caso, el hecho de que las agencias de inteligencia americanas tuvieran acceso de forma generalizada a los datos personales de los ciudadanos europeos puso de relieve que la protección de los mismos no era la adecuada.

Esa excepción nunca debería haberse utilizado en menoscabo de la protección garantizada por la Carta de los Derechos Fundamentales de la UE y el resto de la legislación europea en materia de protección de datos. Recordemos que, de acuerdo con el artículo 52.1 de la Carta, las injerencias en el derecho a la protección de datos de carácter personal son posibles siempre que, respetando el contenido esencial del derecho, se prevean en una norma, respondan a un interés general y sean necesarias y proporcionadas. Estos requisitos deben aplicarse de manera especialmente rigurosa (González Pascual, 2014: 955).

Del mismo modo, la Comisión consideraba que las personas afectadas no disponían de vías jurídicas administrativas o judiciales que les permitían acceder a los datos que les concernían y obtener, en su caso, su rectificación o supresión. Y una normativa que no prevé posibilidad alguna de que el justiciable posea acciones legales para acceder a sus datos personales o para obtener su rectificación o supresión vulnera el contenido esencial del derecho fundamental a la tutela judicial efectiva.

Según reiterada jurisprudencia del Tribunal de Justicia, una normativa que haga posible una injerencia en los derechos fundamentales garantizados por

[20] Véase STJUE, 8 de abril de 2014, Digital Rights Ireland y otros, C- 293/12 y C-594/12, EU:C: 2014:238, apartado 33 y la jurisprudencia ahí citada.

los artículos 7 y 8 de la Carta debe contener reglas claras y precisas que regulen el alcance y la aplicación de una medida e impongan unas exigencias mínimas, de modo que las personas cuyos datos personales resulten afectados dispongan de garantías suficientes que permitan proteger eficazmente sus datos personales contra riesgos de abuso y contra cualquier acceso o utilización ilícitos de los mismos. La necesidad de disponer de esas garantías es aún más importante cuando los datos personales se someten a un tratamiento automático y existe riesgo elevado de acceso ilícito a ellos (Breyer, 2005: 368)[21].

3. El caso Schrems

3.1. Alcance de la sentencia de 6 de octubre de 2015

Maximillian Schrems, un ciudadano austriaco usuario de Facebook desde 2008, cuyos datos personales, como ocurre con los demás usuarios que residen en la UE, se transfieren total o parcialmente desde la filial irlandesa de dicha red social (Facebook Ireland Ltd) a servidores situados en territorio de los Estados Unidos (Facebook Inc.), presentó una reclamación ante la Comisaria para la Protección de Datos irlandesa[22], la autoridad nacional de control.

Según el demandante, a la luz de las revelaciones realizadas en 2013 por Edward Snowden en relación con las actividades de los servicios de información de Estados Unidos (en particular, la National Security Agency o NSA), la normativa y la práctica de este país no garantizaban una protección suficiente de los datos que se le transferían frente a las actividades de vigilancia por las autoridades públicas.

La Comisaria para la Protección de Datos desestimó esa reclamación apreciando que en su Decisión 2000/520/CE la Comisión había constatado que, en el marco del régimen denominado de puerto seguro, Estados Unidos garantizaba un nivel adecuado de protección de los datos personales transferidos.

[21] Véase STUE, 8 de abril de 2014, Digital Rights Ireland y otros, C- 293/12 y C-594/12, EU:C: 2014:238, apartado 54 y 55 y la jurisprudencia ahí citada.
[22] Data Protection Commissioner, el cargo lo ostenta en este momento Helen Dixon.

La defensa de Schrems apeló al Tribunal Supremo de Irlanda que, una vez examinadas las pruebas presentadas por las partes, concluyó que la vigilancia electrónica y la interceptación de los datos personales transmitidos desde la Unión a Estados Unidos servían a finalidades necesarias e indispensables para el interés público[23]. Sin embargo, tomando en consideración las revelaciones del Sr. Snowden, quedaba patente que la NSA y los organismos federales habían cometido "importantes excesos"[24]. Eran precisamente esos "excesos" los que sembraban serias dudas acerca de la pertinencia del nivel de protección estadounidense de los datos personales, tanto conforme a la legislación irlandesa, como en relación con el Derecho de la Unión.

En realidad, en su recurso, el Sr. Schrems impugnaba la licitud del régimen de puerto seguro establecido por esa Decisión de la Comisión, que llevaba a la autoridad nacional de control a desestimar sin investigar su reclamación. Ni se rebatía formalmente la validez de la Directiva 95/46/CE ni la de la Decisión 2000/520/CE.

Así las cosas, la alta instancia judicial irlandesa decidió suspender el procedimiento y plantear al Tribunal de Justicia la cuestión prejudicial (Kokott & Sobotta, 2013: 83). En la sentencia del caso Facebook, el Tribunal de Justicia invalidó la Decisión 2000/520/CE por la que la Comisión, apoyándose en el régimen de puerto seguro, declaraba que las normas americanas garantizaban un nivel adecuado de protección de los datos transferidos desde la Unión a compañías situadas en Estados Unidos.

Pero la sentencia no entró a valorar los principios de puerto seguro porque, a la hora de dictar esa Decisión, la Comisión no comprobó que Estados Unidos garantizara efectivamente un nivel de protección adecuado en razón de su legislación interna o sus compromisos internacionales.

[23] El propio Tribunal Supremo irlandés ya aludió a una justificación específica adecuada para esta clase de vigilancia que "es capaz de afectar gravemente a la tranquilidad y a la reputación pública de cada individuo"; Irish High Court, Kane v. Governor of Mountjoy Prison, 1988, IR 757 769.

[24] En relación con la cantidad de datos que la NSA maneja, un informe del Servicio de Investigación del Congreso de Estados Unidos afirmaba lo siguiente: "Whereas NSA once predicted it was in danger of becoming proverbially deaf due to the spreading use of encrypted communications, it appears that NSA may now be at greater risk of being 'drowned' in information" (Congressional Research Service, 2006: 5).

3.2. Sobre la adecuación de la protección de los datos personales

Sin duda, del artículo 25.6 de la Directiva 95/46/CE se desprende que la Unión pretende asegurar la continuidad de su elevado nivel de protección incluso en caso de transferencia de datos personales a un tercer país[25].

Sin embargo, como ya hemos puesto de relieve, el término "adecuado" significa que no cabe exigir que un tercer país garantice idéntico nivel de protección al del Derecho de la Unión, sino un nivel de protección sustancialmente equivalente al europeo[26]. A falta de esta exigencia, la Unión vería frustrado su objetivo de continuar con un elevado nivel de protección incluso en caso de transferencia de datos personales a un tercer país. Además, el elevado nivel de protección garantizado por la Directiva 95/46/CE entendida a la luz de la Carta de los Derechos Fundamentales de la UE se podría eludir fácilmente con transferencias de datos personales desde la Unión a terceros países para su tratamiento en éstos.

Los medios de los que se sirve ese tercer país para garantizar un nivel de protección sustancialmente equivalente al de la Unión pueden ser diferentes a los aplicados para preservar el cumplimiento de las exigencias de la Directiva 95/46/CE, eso sí, deben ser eficaces para alcanzar el resultado en la práctica (Wolf, 2014: 250).

Por ello, al valorar el nivel de protección ofrecido por un tercer país la Comisión está obligada a apreciar el contenido de las reglas aplicables en ese país, derivadas de la legislación interna o de los compromisos internacionales, así como la práctica seguida para asegurar el cumplimiento de esas reglas, debiendo atender esa institución a todas las circunstancias relacionadas con una transferencia de datos personales a un tercer país.

De igual modo, dado que el nivel de protección garantizado por un tercer país puede evolucionar, incumbe a la Comisión, tras adoptar una decisión conforme al artículo 25.6 de la Directiva 95/46/CE, comprobar periódicamente si sigue

[25] Véase el punto 139 de las conclusiones del abogado general en el caso Facebook.

[26] Llamando la atención sobre la intrusión en la soberanía de los países terceros que esta exigencia supone, Bauchner explica del siguiente modo la adecuación que exige la normativa europea: "While adecuacy is not as strict as equivalency, it nevertheless demands a certain level of aquiescence to (EU) law by thrid-partu countries if they are to continue those relations with Member States" (Bauchner, 2000: 702). Véase también el punto 141 de sus conclusiones del Abogado General en el caso Facebook.

siendo fundada en Derecho y de hecho la constatación sobre el nivel de protección adecuado garantizado por el tercer país en cuestión. En cualquier caso esa comprobación es obligada cuando hay indicios que generan una duda en ese sentido.

Las autoridades nacionales de control y los tribunales nacionales estarán también compelidos a tener en cuenta las circunstancias sobrevenidas después de la adopción de la decisión por parte de la Comisión.

En conclusión, la Comisión no posee el monopolio para apreciar el carácter adecuado del nivel de protección garantizado por un tercer país. Además, cuando adopta una decisión de conformidad con el artículo 25.6 de la Directiva 95/46/CE debe realizar un control estricto de las exigencias del artículo 25 de la misma Directiva, entendida a la luz de las exigencias de la Carta de los Derechos Fundamentales de la UE[27].

Si el sistema de autocertificación no es por sí mismo contrario a lo dispuesto en el artículo 25.6 de la Directiva 95/46/CE, la fiabilidad de este sistema en relación con la exigencia de un nivel de protección adecuado descansa, en esencia, en el establecimiento de mecanismos eficaces de detección y control que permitan identificar y sancionar en la práctica las posibles infracciones de las reglas que garantizan la protección de los derechos fundamentales, en especial del derecho al respeto a la privacidad y a la protección de los datos personales.

3.3. Ausencia de limitación de las injerencias en el derecho a la protección de datos

El sistema que acabamos de analizar se aplica a las entidades privadas pero no a las autoridades públicas de Estados Unidos, cuyas posibles injerencias en los derechos fundamentales de las personas no encuentran límites específicos y definidos. Las exigencias de seguridad nacional, interés público y cumplimiento de la ley permiten dichas injerencias (Seifer, 2008: 10).

Recordemos que, de acuerdo con el artículo 52.1 de la Carta, las injerencias en el derecho a la protección de datos de carácter personal son posibles siempre

[27] Véase, por analogía, STJUE, 8 de abril de 2014, Digital Rights Ireland y otros, C-293/12 y C-594/12, EU:C:2014:238, apartados 47 y 48.

que, respetando el contenido esencial del derecho, se prevean en una norma, respondan a un interés general y sean necesarias y proporcionadas, requisitos estos que deben aplicarse de manera especialmente rigurosa (González Pascual, 2014: 944).

Pero la pregunta que procede hacerse es si realmente existen tales injerencias. Según se desprende de dos Comunicaciones elaboradas en 2013[28], la propia Comisión constató que las autoridades estadounidenses podían acceder a los datos personales transferidos desde los Estados miembros y tratarlos de manera incompatible con las finalidades de esa transferencia, que va más allá de lo estrictamente necesario y proporcionado para la protección de la seguridad nacional. El Parlamento Europeo consideró que el acceso a gran escala de las agencias de inteligencia de Estados Unidos a los datos personales de la UE procesados en virtud del principio de puerto seguro no cumplía los criterios de exención en materia de seguridad nacional[29]. El hecho de que las agencias de inteligencia americanas hubieran tenido acceso de forma generalizada a los datos personales de los ciudadanos europeos ponía de relieve que la protección de los mismos no era la adecuada.

Las excepciones o las limitaciones al derecho a la protección de datos personales no deben exceder de lo estrictamente necesario[30]. Pues bien, no se limita a lo estrictamente necesario una normativa que autoriza de forma generalizada la conservación de la totalidad de los datos personales de todas las personas cuyos datos se hayan transferido desde la Unión a Estados Unidos, sin establecer ninguna diferenciación, limitación o excepción en función del resultado a alcanzar y sin prever ningún criterio objetivo que permita circunscribir el acceso de las autoridades públicas a los datos y su utilización

[28] Comunicación de la Comisión al Parlamento Europeo y al Consejo, de 27 de noviembre de 2013, restablecer la confianza en los flujos de datos entre la Unión Europea y los Estados Unidos de América, COM (2013) 846 final, y Comunicación de la Comisión al Parlamento Europeo y al Consejo, de 27 de noviembre de 2013, sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la Unión y las empresas establecidas en la Unión, COM (2013) 847 final.

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

[30] Véase STJUE, 8 de abril de 2014, Digital Rights Ireland y otros, C- 293/12 y C-594/12, EU:C: 2014:238, apartado 52 y la jurisprudencia ahí citada).

posterior a fines específicos, estrictamente limitados y propios para justificar la injerencia que constituyen tanto el acceso a esos datos como su utilización posterior[31].

La normativa del país tercero debe ofrecer protección jurídica contra posibles arbitrariedades e indicar claramente el alcance de la discrecionalidad y de las potestades de las autoridades públicas.

Del mismo modo, la Comisión consideraba que las personas afectadas no disponían de vías jurídicas administrativas o judiciales que les permitían acceder a los datos que les concernían y obtener, en su caso, su rectificación o supresión. Y una normativa que no prevé posibilidad alguna de que el justiciable posea acciones legales para acceder a sus datos personales o para obtener su rectificación o supresión vulnera el contenido esencial del derecho fundamental a la tutela judicial efectiva.

En lo que atañe al nivel de protección de las libertades y derechos fundamentales garantizado en la Unión, según reiterada jurisprudencia del Tribunal de Justicia, una normativa que haga posible una injerencia en los derechos fundamentales garantizados por los artículos 7 y 8 de la Carta debe contener reglas claras y precisas que regulen el alcance y la aplicación de una medida e impongan unas exigencias mínimas, de modo que las personas cuyos datos personales resulten afectados dispongan de garantías suficientes que permitan proteger eficazmente sus datos personales contra riesgos de abuso y contra cualquier acceso o utilización ilícitos de los mismos (González Fuster, 2014: 37). La necesidad de disponer de esas garantías es aún más importante cuando los datos personales se someten a un tratamiento automático y existe riesgo elevado de acceso ilícito a ellos (Breyer, 2005: 368)[32].

[31] Véase, en este sentido, acerca de la Directiva 2006/24/CE del Parlamento Europeo y del Consejo, de 15 de marzo de 2006, sobre la conservación de datos generados o tratados en relación con las prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modifica la Directiva 2002/58/CE (DO L 105, p. 54), y la STJUE, 8 de abril de 2014, Digital Rights Ireland y otros, C- 293/12 y C-594/12, EU:C: 2014:238, apartados 57 a 61.

[32] Véase STJUE, 8 de abril de 2014, Digital Rights Ireland y otros, C- 293/12 y C-594/12, EU:C: 2014:238, apartado 54 y 55 y la jurisprudencia ahí citada).

El Tribunal de Justicia afirma con rotundidad que "una normativa que permite a las autoridades públicas acceder de forma generalizada al contenido de las comunicaciones electrónicas lesiona el contenido esencial del derecho fundamental al respeto de la vida privada garantizado por el artículo 7 de la Carta"[33] (Ruiz Miguel, 2003: 31). De igual manera, "una normativa que no prevé posibilidad alguna de que el justiciable ejerza acciones en Derecho para acceder a los datos personales que le conciernen o para obtener su rectificación o supresión no respeta el contenido esencial del derecho fundamental a la tutela judicial efectiva que reconoce el artículo 47 de la Carta"[34].

4. Restaurando la confianza en los flujos de datos transatlánticos

4.1. Reacciones e implicaciones prácticas de la sentencia

La trascendencia del asunto Schrems o Facebook, como también se le conoce, ya había comenzado a vislumbrase incluso antes de dictarse la sentencia de 6 de octubre de 2015 (Álvarez Caro & Recio Gayo, 2016: 20). A finales del mes de septiembre la Administración del presidente norteamericano Barack Obama difundió un comunicado poco habitual contra las conclusiones elaboradas por el Abogado General, Yves Bot, considerando que sus afirmaciones eran inexactas y que si en base a ellas se limitaba la transferencia de datos personales de ciudadanos europeos a Estados Unidos, tal cosa iba supuestamente a **"**dañar la protección de los derechos individuales y el libre flujo de información".

Tras conocerse la sentencia y el mismo día de la toma de posesión de los nuevos miembros del Tribunal, la Cámara de Comercio de Estados Unidos en España difundió un alarmante comunicado considerando que la decisión podría nada menos que "interrumpir la actividad empresarial transatlántica, dañar la economía europea y poner en peligro el Mercado Único Digital" puesto que en su opinión, "independientemente de la industria o sector, el libre flujo de datos es un elemento de vital importancia para el desarrollo de la actividad

[33] Apartado 94 de la sentencia, que a su vez se apoya en la STJUE, 8 de abril de 2014, Digital Rights Ireland y otros, C- 293/12 y C-594/12, EU:C: 2014:238, apartado 39.
[34] Apartado 95 de la sentencia.

empresarial en la Unión Europea y contribuye a su crecimiento presente y futuro"[35].

Las reacciones que suscitó en Estados Unidos esta importante sentencia europea pusieron de manifiesto que los datos personales que los ciudadanos tan alegre, gratuita e inconscientemente proporcionamos a los gigantes de Internet norteamericanos haciendo un uso indiscriminado y permanente de sus "servicios", tienen un valor económico y geoestratégico de dimensiones absolutamente desconocidas para la opinión pública.

Pero las alarmas no solo saltaron en aquel lado del Atlántico, en la Unión también se alertó de los efectos perniciosos para la economía de los Estados europeos si los flujos de datos transfronterizos se veían perturbados y no se encontraba una pronta solución que permitiera su restablecimiento[36].

Tras la sentencia que anulaba la Decisión 2000/520/CE, las entidades estadounidenses que se habían acogido al programa de puerto seguro, no tuvieron otro remedio que optar por un nuevo mecanismo de obtención de los datos personales de los ciudadanos europeos, o bien recabando el consentimiento libre y explícito de cada usuario para la transmisión de sus datos, lo cual además de caro y lento resultaba demasiado rígido en un mundo tan versátil y dinámico como el de las comunicaciones electrónicas, o bien a través de cláusulas contractuales tipo, reglas corporativas vinculantes y otros mecanismos similares.

4.2. Puesta al día de los instrumentos de protección de datos en la UE

Uno de los hechos que puede ayudar a una mejor protección de los datos de carácter personal tanto dentro de la Unión, como en las transferencias que se hagan de los mismos a terceros países, es la adopción y posterior entrada en vigor del denominado paquete de reforma de la protección de datos. Este

[35] El comunicado se puede consultar en la siguiente dirección: http://www.amchamspain.com/invalidacion-del-acuerdo-de-puerto-seguro-safe-harbour/

[36] Algunos estudios han apuntado a un descenso del PIB de la UE que podría ir de un -0,8 % a un 1,3% y a una caída de las exportaciones de la UE a Estados Unidos rondaría el -6,7 % debido a la pérdida de competitividad. Véase el estudio del Centro Europeo de Economía Política Internacional para la Cámara de Comercio estadounidense realizado en marzo de 2013: US Chamber of Commerce, The Economic Importance of Getting Data Protection Rights, obtenido el 1 octubre de 2016 de https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf

paquete comprende dos instrumentos distintos: el Reglamento general de protección de datos[37] y una Directiva sobre tratamiento de datos en cuestiones criminales[38]. Ambos instrumentos fueron adoptados el 27 de abril de 2016 y tienen prevista su entrada en vigor dentro de dos años.

Gracias al nuevo Reglamento, las compañías extranjeras que ofrezcan bienes y servicios en la UE deben cumplir con las normas europeas en materia de protección de datos. Aquí surge la incógnita de a qué compañías se les va a exigir ese cumplimiento cuando se trate de empresas matrices estadounidenses cuyas filiales están establecidas en Europa.

Por su parte, la Directiva en cuestiones criminales incluye normas armonizadas para las transferencias de datos en el contexto de la cooperación en materia policial.

Las normas sobre transferencias de datos a terceros países se han reforzado. Tanto el Reglamento como la Directiva aportan reglas claras y detalladas aplicables a los flujos de datos fuera de las fronteras de la Unión que cubren todos los posibles motivos de transmisión: comercial, criminal, entre partes privadas y/o autoridades públicas (Katulic & Vojkovic, 2016: 1447).

Es cierto que la estructura normativa sobre las transferencias de datos hacia terceros Estados continúa siendo muy similar a la contenida en la Directiva 95/46/CE (decisiones de adecuación, cláusulas contractuales tipo y reglas corporativas vinculantes, así como ciertas derogaciones de la prohibición general de transmitir datos fuera de la Unión), pero la reforma clarifica y simplifica estas normas en varios sentidos, a la vez que reduce la burocracia innecesaria. También se incluyen nuevos instrumentos que pueden presidir las transferencias de datos fuera de la UE como los códigos de conducta o la aprobación de mecanismos certificados.

[37] Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), (DO L119, p. 1).

[38] Directiva 2016/680/UE del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, (DO L 119, p. 89).

Las autoridades europeas de control han visto reforzados sus poderes, ya que tanto el Reglamento como la Directiva incluyen expresamente el poder de estas de suspender los flujos de datos hacia receptores fuera de la Unión. El Reglamento, incluso, configura un régimen de sanciones efectivo, armonizando las competencias de las autoridades nacionales de supervisión en este sentido.

Respecto a las decisiones de adecuación que adopta la Comisión, el Reglamento detalla un catálogo preciso de elementos que esta institución europea deberá tener en cuenta cuando evalúe el nivel de protección de datos que ofrece un ordenamiento jurídico de un tercer Estado (normas que regulan el acceso de las autoridades públicas a los datos personales, los derechos de los individuos respecto a sus datos, etc.). Además estas decisiones de adecuación deben ser periódicamente revisadas por la Comisión, al menos cada cuatro años, a fin de comprobar que se siguen respetando los estándares normativos de la UE.

4.3. Reformas normativas estadounidenses que facilitan la negociación

En los últimos meses, el presidente Obama ha tomado algunas iniciativas para revisar diversas normas que pueden afectar al tratamiento de los datos personales.

En primer lugar, se han modificado algunas de las actividades de inteligencia a través de la Directiva 28 sobre política presidencial (PPD-28). Gracias a estas reformas los principios en los que se basa la protección de la privacidad en Estados Unidos pueden extender su aplicación a ciudadanos no americanos. A su vez, otro cambio significativo reside en la forma de recolectar los datos: de un sistema de volcado masivo, las autoridades estadounidenses han pasado a recabar los datos asociados a personas concretas respecto de las que se pueda razonablemente sospechar su implicación en hechos delictivos.

Por otra parte, los programas de vigilancia del gobierno americano han mejorado en el sentido de que se ha reforzado el control judicial, al mismo tiempo que se ha incrementado la transparencia de su uso para el público en general.

ISBN-13: 978-84-16458-41-7 / D.L.: TF-605-2016 / DOI (del libro): 10.4185/cac116

Al aprobarse la Judicial Redress Act se han extendido algunos de los remedios que estaban previstos en la Ley de Privacidad americana solo para los ciudadanos estadounidenses, a los ciudadanos de países "certificados". Gracias a ello, los ciudadanos de los países de la Unión podrán interponer demandas ante los tribunales estadounidenses cuando vean vulnerados su derecho a la protección de datos. Recordemos que hasta este cambio legislativo, la Ley de Privacidad americana solo permitía a sus ciudadanos y a los residentes legales en Estados Unidos acudir a los tribunales para interponer recurso ante la revelación de información personal y su utilización no autorizada por parte de agencias estatales.

5. Adopción de un nuevo acuerdo bilateral para la transferencia de datos: el Escudo de Privacidad

5.1. Principales enmiendas

Las críticas cosechadas por el sistema de puerto seguro junto a la estocada final que significó la sentencia de 6 de octubre de 2015, llevaron a la Comisión y al Departamento de Comercio del Gobierno de Estados Unidos a negociar un nuevo esquema, procurando solventar los problemas que se habían detectado durante los años de vigencia del anterior sistema.

En opinión de la propia Comisión, el nuevo escudo de privacidad proporciona una respuesta firme y efectiva tanto a las recomendaciones que se habían hecho por parte de esta institución antes de la sentencia Schrems, como a las consideraciones contenidas en la propia decisión judicial[39].

Las principales mejoras se dan en torno a las obligaciones que las compañías privadas asentadas en Estados Unidos deben cumplir cuando operan en el territorio de la Unión. Se les va a exigir más transparencia, a la vez que se refuerzan los mecanismos de supervisión. A su vez las transferencias sucesivas hacia terceros Estados se restringen y se dotan de requisitos más estrictos (Von Lewinsky, 2016: 407).

[39] Decisión de Ejecución (UE) 2016/1250 de la Comisión, de 12 de julio de 2016, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por el Escudo de la privacidad UE-EE.UU., DOUE L 207, 1.8.2016, p. 1.

Las obligaciones aplicables a las empresas sujetas al escudo de privacidad están descritas en los "principios de privacidad". Las compañías americanas deben primero adscribirse a este marco en el registro a tal efecto del Departamento de Comercio de los Estados Unidos. Este Departamento es el responsable de gestionar y administrar el escudo de privacidad y de garantizar que las empresas respeten sus compromisos.

Se trata de nuevo, como en el caso del régimen de puerto seguro, de un sistema de autocertificación que se obtiene cuando la empresa acoge los "principios de privacidad" en su política de protección de datos, dándole publicidad en su página web y garantizando los derechos asociados a tal protección. Aquí la novedad radica en que la adhesión al escudo de privacidad debe ser renovada anualmente, con lo que las empresas deben contar con una política de protección de datos acorde con los "principios de privacidad" puesta al día, punto que se había descuidado en el régimen de puerto seguro.

Por tanto, el Departamento de Comercio mantiene actualizada la lista de empresas que forman parte del escudo de privacidad, donde además se pueden consultar el tipo de datos personales que utilizan y la clase de servicios que ofrecen[40]. Las compañías que en un momento dado se acojan al escudo de privacidad pero que después no cumplan con los principios del mismo, aparecerán en otra lista para que los usuarios sepan que no les está permitido recibir datos personales según lo establecido por este sistema. Estas compañías solo podrán guardar los datos anteriormente obtenidos, si se comprometen ante el Departamento de Comercio a tratarlos conforme a los principios asociados al régimen de escudo de privacidad.

Se establecen límites claros y numerosas salvaguardas, incluida supervisión judicial, respecto al acceso a dichos datos por parte de las agencias estatales estadounidenses. El escudo de privacidad garantiza que ese acceso se dará únicamente en la medida en que resulte necesario para lograr un objetivo de interés público, como la seguridad nacional o la aplicación de la ley. Para abordar la cuestión del acceso por organismos estatales se crea la figura del Defensor que recibirá y decidirá sobre las quejas y las dudas que presenten los

[40] Se puede consultar la Lista del Escudo de Privacidad en la web del Departamento de Comercio de EEUU: https://www.privacyshield.gov/welcome

ciudadanos europeos. Este remedio se aplicará a toda transmisión de datos personales a Estados Unidos por razones comerciales.

La protección de los datos de los ciudadanos europeos se hará más efectiva al incrementarse las posibilidades de recurso y, por tanto, de revertir la situación de vulneración y recibir una compensación por los daños sufridos. Las empresas sujetas al escudo de privacidad están obligadas a facilitar un mecanismo de recurso independiente para investigar las reclamaciones no resueltas. Así, cualquier compañía puede optar por el procedimiento de resolución alternativa de litigios en la UE o en Estados Unidos, aunque también podría remitir el caso a la supervisión de una autoridad nacional de protección de datos.

Los ciudadanos podrán dirigirse además a las autoridades nacionales de control, al Departamento de Comercio y a la Comisión Federal del Mercado de Estados Unidos. El acuerdo también crea un panel de resolución de controversias para cuando hayan fracasado las demás opciones de reparación. Y no olvidemos, la nueva figura del Defensor creada solamente a los efectos del amparo de los damnificados por los flujos de datos hacia Estados Unidos.

A parte de estas posibilidades, los ciudadanos europeos, sin necesidad de ser residentes en territorio americano, ahora ya pueden acudir ante los tribunales estadounidenses para solicitar su auxilio en caso de ver vulnerado su derecho a la protección de sus datos personales.

El nuevo acuerdo UE-EEUU prevé una revisión anual, lo que permitirá a la Comisión verificar el buen funcionamiento de todos los aspectos normativos del escudo de privacidad. Nótese que aunque el Reglamento de protección de datos prevé una revisión al menos cada cuatro años de las decisiones de adecuación que adopte la Comisión, aquí se ha querido introducir una garantía adicional rebajando el periodo de verificación a un año.

5.2. Cuestiones que han quedado sin esclarecer

Como ya advirtió el Grupo de Trabajo del Artículo 29, aunque el nuevo escudo de privacidad mejora significativamente el antiguo régimen de puerto seguro,

continúa siendo un sistema muy complejo que adolece en muchas facetas de falta de claridad[41].

El informe presentado por este Grupo de Trabajo también expresaba su preocupación respecto a la configuración del escudo de privacidad tanto en los aspectos relacionados con los flujos comerciales como en las cuestiones que tienen que ver con la seguridad nacional. En este sentido, se hacía notar que no hay una formulación del principio general sobre retención de datos y deducir este principio desde la regulación actual del principio de integridad de los datos y limitación de la finalidad, no resulta tarea fácil.

Quizás esta carencia podrá ser solventada en el futuro a través de una interpretación jurisprudencial adecuada que precise el contenido central del principio. Sin embargo, esta solución ni es la más deseable, ni la más rápida, ni la más segura. Ya que se ha modificado el sistema, se podría haber aprovechado para incluir dicho principio como garantía general. De esa forma, la interpretación posterior solo se habría tenido que preocupar de cuestiones de detalle, no de la construcción desde cero del pilar fundamental del entramado de protección de datos.

Con el fin de aportar más claridad al uso de varias nociones importantes, el Grupo de Trabajo del Artículo 29 sugiere que la UE y Estados Unidos deberían acordar definiciones más claras con las que elaborar un glosario de términos incorporado a la sección FAQ del escudo de privacidad.

En caso de sucesivas transferencias a terceros países no existe una obligación clara de que la legislación de esos Estados tenga que cumplir con determinados requisitos, como por ejemplo que garantice un nivel de protección similar al que exige el escudo de seguridad. Por ello, el Grupo de Trabajo del Artículo 29 concluye que las transmisiones sucesivas de datos no están bien reguladas, especialmente teniendo en cuenta sus objetivos, la limitación de las transferencias y las salvaguardas aplicables a los procesadores de los flujos de datos. Sería conveniente que antes de cada transmisión ulterior a un país tercero, se evaluara cualquier requisito obligatorio

[41] GT29, Dictamen de las Autoridades europeas de protección de datos sobre la decisión de adecuación del Escudo de privacidad, 30 May 2016 (DO L 257, página 8).

de la legislación de dicho país aplicable al importador de los datos para ver si son sustancialmente equivalentes a las exigencias de la normativa europea.

Un punto realmente positivo del nuevo escudo de privacidad es la introducción de otros mecanismos de recurso, aunque en algunas ocasiones estos sean demasiado complejos y difícilmente utilizables por parte de los ciudadanos europeos. El Grupo de Trabajo del Artículo 29 había sugerido que el escudo de privacidad permitiese a las autoridades nacionales de control representar a los ciudadanos de la UE ante los tribunales estadounidenses o, alternativamente, que los individuos pudieran ejercer sus derechos en territorio europeo.

En este sentido, la creación de un Defensor es bienvenida pero habrá que definir muy bien su posición y sus poderes.

En cuanto a los problemas derivados de las necesidades de protección de la seguridad nacional, lo cierto es que el escudo de privacidad no ha descartado completamente la recolección masiva e indiscriminada de datos personales procedentes de la UE por parte de las agencias públicas americanas. La vigilancia masiva e indiscriminada de las personas nunca puede considerarse proporcionada y estrictamente necesaria en una sociedad democrática, tal como se requiere de conformidad con la protección ofrecida a los derechos fundamentales aplicables. Es crucial además que exista una supervisión global de todos los programas de vigilancia (Prislan, 2016: 3).

En mayo de 2016, el Parlamento Europeo a la vista de todos estos aspectos problemáticos aprobó una resolución pidiendo a la Comisión que reabriera las negociaciones con las autoridades estadounidenses sobre el escudo de privacidad[42].

A finales de dicho mes, el Supervisor Europeo de Protección de Datos presentó su opinión acerca del escudo de privacidad, reconociendo los esfuerzos realizados respecto al puerto seguro pero poniendo de relieve que se requería mayores mejoras para conseguir un marco legal sólido y duradero para las

[42] European Parliament, Resolution of 26 May 2016 on transatlantic data flows, 2016/2727(RSP), página 5.

transferencias de datos entre compañías privadas desde la UE a los Estados Unidos[43].

En este sentido, la máxima autoridad europea en la materia que venimos tratando incluyó tres recomendaciones bien definidas: integrar todos los principios de protección de datos, limitar las derogaciones de los mismos, y mejorar las posibilidades de recurso y los mecanismos de supervisión.

6. Conclusiones

En un contexto de globalización creciente y comunicación mundial, la transferencia de datos no está limitada geográficamente, lo que supone un desafío de primer orden a la hora de legislar desde cualquier parte del mundo, cuando no se dispone de un marco jurídico común. Conjugar la diversidad de normativas con la defensa de los derechos fundamentales en la Unión es el desafío al que se enfrentan tanto las instituciones europeas como sus Estados miembros.

Las transferencias de datos personales a terceros países son necesarias, pero ello no obsta para que las mismas ofrezcan un nivel adecuado de protección, ya que cuando esto no es así se interfiere en la vida privada de cada individuo.

La Carta de los Derechos Fundamentales de la UE reconoce el derecho a la protección de datos de carácter personal de forma autónoma, aunque íntimamente ligado a la privacidad. Por su parte, tanto la Directiva 95/46/CE como el nuevo Reglamento general de protección de datos tienen por objeto garantizar la protección de las libertades y de los derechos fundamentales de las personas físicas y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales. Esta legislación permite los flujos de esos datos a terceros países, aunque les exige acreditar un nivel de protección adecuado que, en definitiva, significa un nivel de protección sustancialmente equivalente al que se ofrece en la Unión.

Como las transmisiones de datos a empresas americanas son regulares es importante contar con mecanismos que permitan una constatación rápida y segura de la adecuación del nivel de protección. A esta exigencia respondía el

[43] European Data Protection Supervisor, Opinion 4/2016 on the EU-U.S. Privacy Shield draft adequacy decision, 30 May 2016, página 4.

régimen de puerto seguro configurado por el Departamento de Comercio de Estados Unidos y avalado por la Comisión en su Decisión 2000/520/CE. Sin embargo, la noticia de los programas de vigilancia masiva por parte de las agencias estatales estadounidenses, que se sirvieron de los datos exportados a las sedes centrales de compañías como Facebook, Apple o Google, encendió todas las alarmas, propiciando reclamaciones como la que se encuentra en el origen de la sentencia de 6 de octubre de 2015, que dio al traste con la decisión de adecuación mencionada y con propio sistema de puerto seguro.

En su lugar, la Comisión Europea y el Departamento de Comercio de Estados unidos han negociado un nuevo régimen denominado escudo de privacidad. En el actual contexto internacional, con el surgimiento del big data y las crecientes exigencias de seguridad, el alcance y la dimensión de la recopilación y el uso de datos personales se han incrementado espectacularmente desde que se promulgara la Decisión 520/2000/CE. Así las cosas, el escudo de privacidad presenta mejoras significativas respeto al anterior sistema. La protección que otorga es esencialmente equivalente a la de la legislación europea en vigor, manteniendo lo sustancial de sus principios fundamentales.

Si bien esto es verdad, hay que poner de relieve como algunos de los principios clave de la protección de datos en la UE no están reflejados en la nueva Decisión de adecuación o han sido sustituidos por nociones alternativas que pueden acarrear problemas en la práctica.

En definitiva, el escudo de privacidad como solución concertada para los flujos de datos transatlánticos impone mayores exigencias a las compañías estadounidenses para la protección de los datos personales de los ciudadanos europeos, aunque todavía sería susceptible de mejoras significativas.

La revolución digital ha llevado a que tanto los gobiernos como las empresas de ambos lados del Atlántico asuman nuevos retos, a la vez que obligan a sus autoridades a cooperar. Washington y Bruselas tienen muchos valores e intereses en común, aunque en ocasiones muestren diferentes puntos de vista a la hora de afrontar retos tecnológicos como la privacidad de los consumidores o la ciberseguridad. El desafío radica en encontrar los puntos de encuentro

ISBN-13: 978-84-16458-41-7 / D.L.: TF-605-2016 / DOI (del libro): 10.4185/cac116

entre ambas visiones para construir una asociación estratégica digital, sin sacrificar la protección de los derechos fundamentales.

7. Referencias bibliográficas

M Álvarez Caro, M Recio Gay (2015): "Hacia un acuerdo Safe Harbour renovado para la transferencia internacional de datos entre EE.UU. y la UE", en *Working Papers on European Law and Regional Integration*, 25, páginas 1 a 26.

J Bauchner (2000): "State Sovereignty and the Globalizing Effects of the Internet: A Case Study of the Privacy Debate", en *Brooklyn Journal of International Law*, 26, páginas 689 a 722.

P Blume (2000): ""Transborder data flow: Is there a solution in sight?", en *International Journal of Law and Information Technology*, 8-1, páginas 65 a 86.

P Breyer (2005): "Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR", en *European Law Journal*, 11-3, páginas 365 a 375.

L Colonna (2014): "Article 4 of the EU Data Protection Directive and the irrelevance of the EU-US Safe Harbor Program?", en *International Data Privacy Law*, 4-3, páginas 203 a 221.

Comisión Europea (2016): *Guía acerca del Escudo de Privacidad UE-EE.UU.* Bruselas: Unión Europea.

G González Fuster (2014): *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Heidelberg: Springer.

M González Pascual (2014): "El TJUE como garante de los derechos de la UE a la luz de la sentencia Digital Rights Ireland", en *Revista de Derecho Comunitario Europeo*, 49, páginas 943 a 971.

D Greer (2011): "Safe Harbor – A Framework That Works", en *International Data Privacy Law*, 1-3, páginas 143 a 148.

T Katulic, G Vojkovic (2016): "From Safe Harbor to European Data Protection Reform", en *MIPRO*, 30, páginas 1447 a 1451.

J Kokott, C Sobotta (2013): “The Distinction between privacy and data protection in the jurisprudence of the CJEU and the ECHR”, en *International Data Privacy Law*, 3-4, páginas 83 a 95.

C Kuner (2013): *Transborder Data Flows and Data Privacy Law*. Oxford: Oxford University Press.

N Prislan (2016): “¿Existe una grieta digital entre EEUU y la UE?”, en *Política Exterior*, 172, páginas 1 a 7.

C Ruiz Miguel (2003): “El derecho a la protección de datos personales en la Carta de Derechos Fundamentales de la Unión Europea: análisis crítico”, en *Revista de Derecho Comunitario Europeo*, 14, páginas 7 a 43.

J Seifer (2008): *Data Mining and Homeland Security: An Overview*. Washington: Congressional Research Service report RL31798, Library of Congress.

K Von Lewinski (2016): “Privacy Shield – Notdeich nach Pearl Harbor für die transatlantischen Datentransfers”, en *Europarecht*, 4, páginas 405 a 420.

C Wolf (2014): “Delusions of Adequacy? Examinig the Case for Finding the United States Adequate for Cross-Border EU-US Data Transfers”, en *Washington University Journal of Law & Policy*, 43, páginas 227 a 257.