COMISIÓN
EUROPEA

Bruselas, 27.11.2013
COM(2013) 846 final

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO

Restablecer la confianza en los flujos de datos entre la UE y EE.UU.

1. INTRODUCCIÓN: EL ENTORNO CAMBIANTE DEL FLUJO DE DATOS ENTRE LA UE Y EE.UU.

La Unión Europea y los Estados Unidos son socios estratégicos, y esta asociación es fundamental para la promoción de nuestros valores compartidos, nuestra seguridad y nuestro liderazgo común en los asuntos mundiales.

Sin embargo, la confianza en la asociación se ha visto afectada negativamente y debe restablecerse. La UE, sus Estados miembros y los ciudadanos europeos han manifestado una gran preocupación por la revelación de la existencia de programas de recogida de información a gran escala por parte de los Estados Unidos, en especial en lo que se refiere a la protección de los datos personales[1]. La vigilancia masiva de las comunicaciones privadas, ya se trate de los ciudadanos, las empresas o los dirigentes políticos, es inaceptable.

Las transferencias de datos personales son un elemento importante y necesario de la relación transatlántica. Forman parte integrante de los intercambios comerciales entre ambos lados del Atlántico, incluidos los relacionados con los nuevos sectores digitales en crecimiento, tales como las redes sociales o la computación en nube, que implican la transferencia de grandes cantidades de datos de la UE a los Estados Unidos. Constituyen asimismo un componente esencial de la cooperación entre los servicios con funciones coercitivas de la UE y los Estados Unidos, así como de la cooperación entre los Estados miembros y los Estados Unidos en el ámbito de la seguridad nacional. A fin de facilitar los flujos de datos y garantizar al mismo tiempo un nivel elevado de protección conforme a la legislación de la UE, los Estados Unidos y la UE han establecido una serie de acuerdos y arreglos.

Los intercambios comerciales son objeto de la Decisión 2000/520/CE[2] (en lo sucesivo, «la Decisión de puerto seguro»). Dicha Decisión establece una base jurídica para la transferencia de datos personales desde la UE a las empresas establecidas en los Estados Unidos que se han adherido a los principios del régimen de puerto seguro.

El intercambio de datos personales entre la UE y los Estados Unidos a los efectos de la aplicación de la ley, incluido el relacionado con la prevención y la lucha contra el terrorismo y otras formas graves de delincuencia, se rige por una serie de acuerdos a escala de la UE. Dichos acuerdos son el Acuerdo de Asistencia Judicial Mutua[3], el Acuerdo sobre la utilización y la transferencia de los registros de nombres de los pasajeros (PNR)[4], el Acuerdo relativo al tratamiento y la transferencia de datos de mensajería financiera a efectos del Programa de Seguimiento de la Financiación del Terrorismo (TFTP)[5], y el Acuerdo entre

---

1 A los efectos de la presente Comunicación, las referencias a los ciudadanos de la UE incluyen también a los nacionales de terceros países que entran dentro del ámbito de aplicación de la legislación de protección de datos de la Unión Europea.

2 Decisión de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América (DO L 215 de 25.8.2000, p. 7).

3 Decisión 2009/820/PESC del Consejo, de 23 de octubre de 2009, sobre la celebración, en nombre de la Unión Europea, del Acuerdo de Extradición entre la Unión Europea y los Estados Unidos de América y del Acuerdo de Asistencia Judicial en materia penal entre la Unión Europea y los Estados Unidos de América (DO L 291 de 7.11. 2009, p. 40).

4 Decisión del Consejo, de 26 de abril de 2012, relativa a la celebración del Acuerdo entre los Estados Unidos de América y la Unión Europea sobre la utilización y la transferencia de los registros de nombres de los pasajeros al Departamento de Seguridad del Territorio Nacional de los Estados Unidos (DO L 215 de 11.8.2012, p. 4).

5 Decisión del Consejo, de 13 de julio de 2010, relativa a la celebración del Acuerdo entre la Unión Europea y los Estados Unidos de América relativo al tratamiento y la transferencia de datos de mensajería financiera de la Unión Europea a los Estados Unidos a efectos del Programa de Seguimiento de la Financiación del Terrorismo (DO L 195 de 27.7.2010, p. 3).

Europol y los Estados Unidos. Estos acuerdos responden a desafíos importantes en materia de seguridad y satisfacen los intereses de seguridad comunes de la UE y de los Estados Unidos, a la vez que proporcionan un elevado nivel de protección de los datos personales. Además, la UE y los Estados Unidos están negociando actualmente un acuerdo marco sobre la protección de datos en el ámbito de la cooperación policial y judicial (en lo sucesivo «el Acuerdo Marco»)[6]. El objetivo es lograr un elevado nivel de protección de datos para los ciudadanos cuyos datos se intercambian, con lo que se seguirá avanzando en la cooperación entre la UE y los Estados Unidos en la lucha contra la delincuencia y el terrorismo sobre la base de los valores compartidos y las garantías acordadas.

Estos instrumentos se aplican en un entorno en el que los flujos de datos personales están adquiriendo cada vez más importancia.

Por una parte, el desarrollo de la economía digital ha dado lugar a un crecimiento exponencial de la cantidad, calidad, diversidad y naturaleza de las actividades de tratamiento de datos. Ha aumentado el uso de los servicios de comunicación electrónica por parte de los ciudadanos en su vida cotidiana. Los datos personales se han convertido en un activo de gran valor: el valor estimado de los datos de los ciudadanos de la UE fue de 315 000 millones EUR en 2011 y tiene un potencial de crecimiento de casi 1 billón EUR al año hasta 2020[7]. El mercado de análisis de grandes conjuntos de datos está aumentando en un 40 % anual a nivel mundial[8]. Del mismo modo, la evolución tecnológica, por ejemplo la relacionada con la computación en nube, pone en perspectiva la noción de transferencia internacional de datos a medida que los flujos transfronterizos de datos se están convirtiendo en una realidad cotidiana.[9]

El aumento del uso de las comunicaciones electrónicas y los servicios de tratamiento de datos, incluida la computación en nube, también ha ampliado considerablemente el alcance y la importancia de las transferencias transatlánticas de datos. Elementos como la posición central de las empresas estadounidenses en la economía digital[10], el tráfico transatlántico de una gran parte de las comunicaciones electrónicas y el volumen de los flujos de datos electrónicos entre la UE y los Estados Unidos son cada vez más importantes.

Por otra parte, los métodos modernos de tratamiento de los datos personales plantean cuestiones nuevas e importantes. Ello se aplica tanto a las nuevas formas de tratamiento a gran escala de los datos de los consumidores por empresas privadas con fines comerciales como a la mayor capacidad de vigilancia a gran escala de los datos de las comunicaciones por los servicios de información.

Los programas estadounidenses de recopilación de información a gran escala, como PRISM, afectan a los derechos fundamentales de los ciudadanos europeos y, en particular, a su derecho a la privacidad y a la protección de los datos personales. Estos programas también apuntan a una conexión entre la vigilancia gubernamental y el tratamiento de los datos por parte de las empresas privadas, especialmente las empresas estadounidenses de internet.

---

6 El Consejo adoptó el 3 de diciembre de 2010 la Decisión por la que se autoriza a la Comisión a negociar este Acuerdo (véase el IP/10/1661 de 3 de diciembre de 2010).

7 Véase Boston Consulting Group, «The Value of our Digital Identity (El Valor de Nuestra Identidad Digital)», noviembre de 2012.

8 Véase McKinsey, «Big data: The next frontier for innovation, competition and productivity (Grandes datos: la última frontera para la innovación, la competencia y la productividad), 2011»;

9 Comunicación de 2001 «Liberar el potencial de la computación en nube en Europa» [COM(2012) 529 final].

10 Por ejemplo, el total agregado de visitantes únicos de países europeos a Microsoft Hotmail, Google Gmail y Yahoo! Mail en junio de 2012 superó los 227 millones, eclipsando a todos los demás proveedores. El total agregado de usuarios únicos europeos que accedieron a Facebook y Facebook Mobile en marzo de 2012 fue de 196,5 millones, con lo que Facebook fue la red social más grande en Europa. Google es el primer motor de búsqueda de internet: cuenta con el 90,2 % de los usuarios de internet a nivel mundial. El servicio estadounidense de mensajería móvil What's App fue utilizado por el 91 % de los usuarios de iPhone de Alemania en junio de 2013.

Como consecuencia de ello, pueden tener un impacto económico. Si a los ciudadanos les preocupa el tratamiento a gran escala de sus datos personales por parte de las empresas privadas o la supervisión de tales datos por los servicios de información cuando utilizan internet, puede resultar afectada su confianza en la economía digital, con las posibles consecuencias negativas en el crecimiento.
Esta evolución plantea nuevos retos en cuanto a los flujos de datos entre la Unión Europea y los Estados Unidos. La presente Comunicación responde a esos retos. Estudia la manera de avanzar sobre la base de las conclusiones del informe de los copresidentes de la UE del grupo de trabajo *ad hoc* UE-EE.UU. y de la Comunicación sobre el puerto seguro.
Su objetivo es proporcionar una forma eficaz de restablecer la confianza y reforzar la cooperación entre la UE y los Estados Unidos en estos ámbitos y fortalecer las relaciones transatlánticas en general.

La presente Comunicación parte de la premisa de que el nivel de protección de los datos personales debe abordarse en su contexto adecuado, sin que ello afecte a las demás vertientes de las relaciones entre la UE y los Estados Unidos, incluidas las negociaciones en curso con vistas a una Asociación Transatlántica de Comercio e Inversión. Por este motivo, los niveles de protección de datos no se negociarán en el marco de la Asociación Transatlántica de Comercio e Inversión, que respetará plenamente las normas de protección de datos.

Es importante señalar que, si bien la UE puede actuar en ámbitos de su competencia, en especial con objeto de garantizar la aplicación de su legislación[11], la seguridad nacional sigue siendo competencia exclusiva de cada Estado miembro[12].

2. EFECTOS EN LOS INSTRUMENTOS DE TRANSFERENCIA DE DATOS

En primer lugar, en lo que respecta a los datos transferidos con fines comerciales, el régimen de puerto seguro ha resultado ser un vehículo importante de transferencia de datos entre la Unión Europea y los Estados Unidos. Su importancia comercial ha ido en aumento a medida que los flujos de datos personales han ido cobrando mayor importancia en las relaciones comerciales transatlánticas. En los últimos trece años, el régimen de puerto seguro ha evolucionado hasta incluir más de 3 000 empresas, más de la mitad de las cuales se han adherido al mismo en los últimos cinco años. Sin embargo, ha aumentado la preocupación por el nivel de protección de los datos personales de los ciudadanos de la UE transferidos a los Estados Unidos en el marco del régimen de puerto seguro. El carácter voluntario y declarativo del régimen ha centrado la atención en su transparencia y cumplimiento. Si bien la mayoría de las empresas estadounidenses aplican sus principios, algunas empresas autocertificadas no lo hacen. La no aplicación por parte de algunas empresas autocertificadas de los principios de puerto seguro, que protegen la privacidad, coloca a dichas empresas en situación de ventaja competitiva respecto a las empresas europeas que operan en los mismos mercados.
Además, dado que en el marco del régimen de puerto seguro se permiten limitaciones a las normas de protección de datos en caso de que sean necesarias por motivos de seguridad nacional[13], se ha planteado la cuestión de si la recogida y el tratamiento a gran escala de información personal en el marco de los programas de vigilancia de los Estados Unidos son necesarios y proporcionados en interés de la seguridad nacional. Por otro lado, se desprende claramente de las conclusiones del grupo de trabajo *ad hoc* UE-EE.UU. que, en el marco de

[11] Véase la sentencia del Tribunal de Justicia de la Unión Europea en el asunto C-300/11, ZZ contra Secretary of State for the Home Department.
[12] Artículo 4, apartado 2, del TUE.
[13] Véase, por ejemplo, la Decisión de puerto seguro, anexo I.

estos programas, los ciudadanos de la UE no gozan de los mismos derechos y las mismas garantías procesales que los estadounidenses.

El alcance de estos programas de vigilancia, combinado con la desigualdad de trato de los ciudadanos de la UE, pone en cuestión el nivel de protección que ofrece el régimen de puerto seguro. Las autoridades estadounidenses pueden acceder y seguir tratando los datos personales de los ciudadanos de la UE enviados a los Estados Unidos en el marco del régimen de puerto seguro de forma incompatible con los motivos por los que se recogieron inicialmente dichos datos en la UE y con los fines por los que se transfirieron a los Estados Unidos. La mayoría de las empresas estadounidenses de internet relacionadas más directamente con estos programas están certificadas en el marco del régimen de puerto seguro.

En segundo lugar, por lo que se refiere a los intercambios de datos con fines coercitivos, los acuerdos vigentes (PNR, TFTP) han resultado ser herramientas muy valiosas para hacer frente a amenazas comunes a la seguridad relacionadas con la delincuencia transnacional grave y el terrorismo, al tiempo que establecen garantías de un nivel elevado de protección de datos[14]. Dichas garantías se extienden a los ciudadanos de la UE, y los acuerdos contemplan mecanismos para revisar su aplicación y abordar las cuestiones que son motivo de preocupación. El Acuerdo TFTP también establece un sistema de supervisión, en el que supervisores independientes de la UE comprueban el modo en que los Estados Unidos buscan datos que entran en el ámbito del Acuerdo.

Ante la inquietud despertada en la UE por los programas de vigilancia estadounidenses, la Comisión Europea ha hecho uso de estos mecanismos para comprobar cómo se aplican los acuerdos. En el caso del acuerdo PNR, se llevó a cabo una revisión conjunta, con la participación de expertos en protección de datos de la UE y de los Estados Unidos, en la que se examinó la manera en que se ha aplicado el Acuerdo[15]. En dicha revisión no se observó ningún indicio de que los programas de vigilancia estadounidenses se apliquen también o afecten a los datos de los pasajeros regulados por el Acuerdo PNR. En el caso del Acuerdo TFTP, la Comisión evacuó consultas formales a raíz de las alegaciones de que los servicios de información estadounidenses accedían directamente a los datos personales en la UE, infringiendo el Acuerdo. Dichas consultas no pusieron de manifiesto ningún elemento que demostrase una vulneración del Acuerdo TFTP e indujeron a los Estados Unidos a proporcionar garantías por escrito de que no se habían recopilado datos directamente en infracción del Acuerdo.

Sin embargo, la recogida y el tratamiento a gran escala de información personal en el marco de los programas de vigilancia exigen mantener un control muy riguroso de la aplicación de los Acuerdos PNR y TFTP en el futuro. Por ello, la UE y los Estados Unidos han acordado avanzar la próxima revisión conjunta del Acuerdo TFTP, que se celebrará en la primavera de 2014. En dicha revisión y en las revisiones futuras se garantizará una mayor transparencia sobre el funcionamiento del sistema de supervisión y la protección de los datos de los ciudadanos de la UE. Al mismo tiempo, se adoptarán medidas para garantizar que el sistema de supervisión siga prestando gran atención al modo en que se tratan los datos transferidos a los Estados Unidos conforme al Acuerdo, centrándose especialmente en el modo en que esos datos son compartidos entre las autoridades estadounidenses.

---

[14] Véase el informe conjunto de la Comisión y del Departamento del Tesoro estadounidense sobre el valor de los datos facilitados en el ámbito del TFTP, con arreglo al artículo 6, apartado 6, del Acuerdo entre la Unión Europea y los Estados Unidos de América relativo al tratamiento y la transferencia de datos de mensajería financiera de la Unión Europea a los Estados Unidos a efectos del Programa de Seguimiento de la Financiación del Terrorismo.

[15] Véase el informe de la Comisión «Revisión conjunta de la ejecución del Acuerdo entre la Unión Europea y los Estados Unidos de América sobre el tratamiento y la transferencia de los registros de nombres de los pasajeros al Departamento de Seguridad del Territorio Nacional de los Estados Unidos».

En tercer lugar, el aumento del volumen de tratamiento de datos personales subraya la importancia de las garantías legales y administrativas aplicables. Uno de los objetivos del grupo de trabajo *ad hoc* UE-EE.UU. era determinar qué garantías debían aplicarse para minimizar el impacto del tratamiento en los derechos fundamentales de los ciudadanos de la UE. También son necesarias garantías para proteger a las empresas. Determinadas leyes estadounidenses, como la «Patriot Act», permiten a las autoridades estadounidenses pedir directamente a las empresas acceso a los datos almacenados en la UE. Por consiguiente, puede ocurrir que se pida a las empresas europeas, y a las empresas estadounidenses presentes en la UE, que transfieran datos a los Estados Unidos en incumplimiento de la legislación de la UE y de los Estados miembros, por lo que dichas empresas se enfrentan a un conflicto de obligaciones legales. La inseguridad jurídica que resulta de esas peticiones directas puede frenar el desarrollo de nuevos servicios digitales, como la computación en nube, que pueden proporcionar soluciones eficientes y de menor coste para las personas y las empresas.

3. GARANTÍA DE LA EFICACIA DE LA PROTECCIÓN DE DATOS

Las transferencias de datos personales entre la Unión Europea y los Estados Unidos son un componente esencial de las relaciones comerciales transatlánticas. El intercambio de información es también un componente esencial de la cooperación en materia de seguridad entre la UE y los Estados Unidos, de vital importancia para el objetivo común de la prevención y la lucha contra las formas graves de delincuencia y el terrorismo. No obstante, las revelaciones recientes sobre los programas estadounidenses de recogida de información han afectado negativamente a la confianza en la que se basa dicha cooperación. En particular, han afectado a la confianza en los métodos de tratamiento de datos personales. Deben adoptarse las siguientes medidas para restablecer la confianza en las transferencias de datos en beneficio de la economía digital, la seguridad, tanto en la UE como en los Estados Unidos, y las relaciones transatlánticas en general.

3.1. Reforma de la protección de datos de la UE

La reforma en materia de protección de datos propuesta por la Comisión en enero de 2012[16] representa una respuesta clave en cuanto a la protección de los datos personales. El paquete de protección de datos propuesto consta de cinco componentes de especial importancia.

En primer lugar, por lo que se refiere al ámbito de aplicación territorial, la propuesta de Reglamento establece claramente que las empresas que no están establecidas en la Unión tendrán que aplicar la normativa de protección de datos de la UE cuando ofrezcan bienes y servicios a los consumidores europeos u observen su comportamiento. En otras palabras, se respetará el derecho fundamental a la protección de datos, con independencia de la ubicación geográfica de una empresa o de los locales en que efectúe el tratamiento de los datos[17].

En segundo lugar, en cuanto a las transferencias internacionales, el Reglamento propuesto establece las condiciones en las que los datos pueden transferirse fuera de la UE. Las

---

16 COM(2012) 10 final: Propuesta de Directiva del Parlamento Europeo y del Consejo 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, Bruselas, 25.1.2012; COM(2012) 11 final: Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos).

17 La Comisión toma nota de que el Parlamento Europeo confirmó y reforzó este principio importante, consagrado en el artículo 3 del Reglamento propuesto, en su votación de 21 de octubre de 2013 sobre los informes de reforma en materia de protección de datos de los europarlamentarios Jan-Philipp Albrecht y Dimitrios Droutsas de la Comisión de Libertades Civiles, Justicia y Asuntos de Interior (LIBE).

transferencias solo pueden permitirse cuando se cumplen tales condiciones[18], que garantizan un elevado nivel de protección de los derechos individuales.

En tercer lugar, en cuanto a la aplicación de la ley, las normas propuestas disponen sanciones proporcionadas y disuasorias (hasta el 2 % del volumen de negocios mundial anual de una empresa) a fin de asegurarse de que las empresas se atienen a la legislación de la UE[19]. La existencia de sanciones creíbles inducirá en mayor medida a las empresas a cumplir la legislación de la UE.

En cuarto lugar, el Reglamento propuesto contiene normas claras sobre las obligaciones y responsabilidades de los encargados del tratamiento de datos, como los proveedores de servicios de computación en nube, en particular en materia de seguridad[20]. Como han puesto de manifiesto las revelaciones sobre los programas estadounidenses de recogida de información, ello es de suma importancia porque estos programas afectan a los datos almacenados en la nube. Asimismo, las empresas que suministran espacio de almacenamiento en la nube a las que se pide que faciliten datos personales a autoridades extranjeras no podrán eludir su responsabilidad en su condición de encargados en lugar de responsables del tratamiento de datos.

En quinto lugar, el paquete conducirá al establecimiento de normas completas para la protección de los datos personales tratados en el sector de la ejecución de la ley.

Se espera que se apruebe el paquete en el momento oportuno a lo largo de 2014[21].

3.2. Hacer más seguro el régimen de puerto seguro

El régimen de puerto seguro es un componente importante de las relaciones comerciales entre la UE y los Estados Unidos, en el que se apoyan las empresas de ambos lados del Atlántico.

En el informe de la Comisión sobre el funcionamiento del régimen de puerto seguro se señalan una serie de deficiencias del mismo. Como consecuencia de la falta de transparencia y de control de su ejecución, algunas empresas autocertificadas que se han adherido al régimen de puerto seguro no cumplen, en la práctica, sus principios. Ello ha tenido un impacto negativo en los derechos fundamentales de los ciudadanos de la UE. Asimismo, crea una desventaja para las empresas europeas con respecto a las empresas competidoras estadounidenses que operan en el marco del régimen, pero en la práctica no aplican sus principios. Esta deficiencia afecta también a la mayoría de las empresas estadounidenses que aplican correctamente el régimen. El régimen de puerto seguro sirve asimismo de interfaz para la transferencia de los datos personales de los ciudadanos de la UE desde la UE a los Estados Unidos por parte de las empresas las que se pide que suministren datos a los servicios de información de los Estados Unidos en el marco de los programas de recogida de información de los Estados Unidos. Si no se corrigen, estas deficiencias generan una

---

[18] La Comisión toma nota de que, en su votación de 21 de octubre de 2013, la Comisión LIBE del Parlamento Europeo propuso incluir una disposición en el Reglamento futuro que supeditara las peticiones de las autoridades extranjeras de acceso a datos personales recogidos en la UE a la obtención de una autorización previa de una autoridad nacional de protección de datos en caso de que la petición correspondiente se realizara al margen de un tratado de asistencia jurídica mutuo u otro acuerdo internacional.

[19] La Comisión toma nota de que en su votación de 21 de octubre de 2013, la Comisión LIBE propuso reforzar la propuesta de la Comisión estableciendo que las multas puedan ascender al 5 % del volumen de negocios mundial anual de una empresa.

[20] La Comisión toma nota de que, en su votación de 21 de octubre de 2013, la Comisión LIBE apoyó el refuerzo de las obligaciones y responsabilidades de los procesadores de datos, en especial en relación con el artículo 26 del Reglamento propuesto.

[21] En las conclusiones del Consejo Europeo de octubre de 2013 se señala: «Es importante fomentar la confianza de los ciudadanos y de las empresas en la economía digital. La adopción a su debido tiempo de un sólido marco general de la UE para la protección de datos y de la Directiva sobre ciberseguridad es esencial para la realización del Mercado Único Digital para 2015».

desventaja competitiva para las empresas de la UE con un impacto negativo en el derecho fundamental a la protección de los datos personales de los ciudadanos de la UE.

Las deficiencias del régimen de puerto seguro se subrayaron en la respuesta de las autoridades europeas de protección de datos a las recientes revelaciones sobre la vigilancia. El artículo 3 del régimen de puerto seguro autoriza a dichas autoridades a suspender, en determinadas condiciones, los flujos de datos a empresas certificadas.[22] Los comisarios alemanes responsables de la protección de datos han decidido no expedir nuevos permisos para las transferencias de datos a países terceros (por ejemplo, para el uso de determinados servicios de computación en nube). Examinarán también si deben suspenderse las transferencias de datos sobre la base del régimen de puerto seguro.[23] Existe el riesgo de que tales medidas, adoptadas a nivel nacional, creen diferencias de cobertura, lo que significa que el régimen de puerto seguro dejaría de ser un mecanismo central para la transferencia de datos personales entre la UE y los Estados Unidos.

Con arreglo a la Directiva 95/46/CE, la Comisión tiene la potestad de suspender o derogar la Decisión de puerto seguro si el régimen ya no proporciona un nivel de protección adecuado. Además, el artículo 3 de la Decisión de puerto seguro establece que la Comisión podrá derogar, suspender o limitar el ámbito de aplicación de la Decisión, mientras que, con arreglo al artículo 4, la Comisión podrá adaptar la Decisión en cualquier momento de conformidad con la experiencia resultante de su aplicación.

En este contexto, pueden tomarse en consideración diversas opciones, como las siguientes:

- mantener el *statu quo*;
- reforzar el régimen de puerto seguro y revisar a fondo su funcionamiento;
- suspender o derogar la Decisión de puerto seguro.

Habida cuenta de las deficiencias halladas, no puede mantenerse la aplicación actual del régimen de puerto seguro. Sin embargo, su derogación afectaría negativamente a los intereses de las empresas de la UE y de los Estados Unidos que se han adherido al mismo. La Comisión considera que debería reforzarse dicho régimen.

Deben subsanarse las deficiencias estructurales relacionadas con la transparencia y la aplicación y deben reforzarse los principios sustantivos del régimen de puerto seguro y la aplicación de la excepción por motivos de seguridad nacional.

Más concretamente, para que el régimen de puerto seguro funcione según lo previsto, el seguimiento y la supervisión por parte de las autoridades estadounidenses del cumplimiento de las empresas certificadas de los principios de puerto seguro deben ser más eficaces y sistemáticos. Debe mejorarse la transparencia de las políticas de privacidad de las empresas certificadas. Asimismo, debe garantizarse a los ciudadanos de la UE la disponibilidad de mecanismos de solución de litigios y su acceso.

Con carácter de urgencia, la Comisión debatirá con las autoridades de los Estados Unidos las deficiencias detectadas. Las soluciones deberán hallarse antes del final del verano de 2014 y aplicarse lo antes posible. Sobre esa base, la Comisión realizará un balance completo del funcionamiento del régimen de puerto seguro. Este proceso más amplio de revisión debería

---

[22] En concreto, de conformidad con el artículo 3 de la Decisión de puerto seguro, estas suspensiones pueden producirse en los casos en que: existen grandes probabilidades de que se estén vulnerando los principios; razones para creer que el mecanismo de aplicación correspondiente no ha tomado o no tomará las medidas oportunas y adecuadas 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 de los Estados miembros de la UE han hecho esfuerzos razonables en estas circunstancias para notificárselo a la entidad y proporcionarle la oportunidad de alegar.

[23] «Bundesbeauftragten für den Datenschutz und die Informationsfreiheit», comunicado de prensa de 24 de julio de 2013.

implicar una consulta abierta y un debate en el Parlamento Europeo y el Consejo, así como conversaciones con las autoridades estadounidenses.
También es importante que la excepción por motivos de seguridad nacional prevista en la Decisión de puerto seguro solo se utilice en la medida en que sea estrictamente necesaria y proporcionada.

3.3. Fortalecer las garantías en materia de protección de datos en el marco de la cooperación entre los servicios con funciones coercitivas

La UE y los Estados Unidos están negociando actualmente un acuerdo marco de protección de datos sobre la transferencia y el tratamiento de datos personales en el contexto de la cooperación policial y judicial en asuntos penales. La celebración de tal acuerdo, que proporciona un elevado nivel de protección de los datos personales, representaría una gran contribución al refuerzo de la confianza a ambos lados del Atlántico. La mejora de la protección de los derechos de los ciudadanos de la UE en esta materia contribuiría a reforzar la cooperación transatlántica en la prevención y la lucha contra la delincuencia y el terrorismo.
De conformidad con la Decisión por la que se autoriza a la Comisión a negociar el acuerdo marco, el objetivo de las negociaciones debe ser garantizar un elevado nivel de protección de conformidad con el acervo de la UE en materia de protección de datos. Ello debería reflejarse en la adopción de normas y garantías relativas, entre otras cosas, a la limitación de los fines, a las condiciones y la duración de la conservación de los datos. En el contexto de la negociación, la Comisión también debe obtener compromisos sobre los derechos exigibles, incluidos los mecanismos de recurso judicial para los ciudadanos de la UE que no residen en los Estados Unidos[24]. La estrecha cooperación entre la UE y los Estados Unidos para abordar retos comunes en materia de seguridad deberá traducirse en esfuerzos para garantizar que los ciudadanos gocen de los mismos derechos cuando se traten los mismos datos para los mismos fines a ambos lados del Atlántico. También es importante que se definan claramente las excepciones por motivos de seguridad nacional. A este respecto, deberán acordarse garantías y limitaciones.
Estas negociaciones brindan la oportunidad de aclarar que los datos personales conservados por empresas privadas y situadas en la UE no serán directamente accesibles ni se transferirán a los servicios con funciones coercitivas fuera de los canales formales de cooperación, como los acuerdos de asistencia jurídica mutua o los acuerdos sectoriales UE-EE.UU. que autoricen tales transferencias. Debe quedar excluido el acceso por otros medios, a menos que este se

[24] Véase el fragmento correspondiente del comunicado de prensa conjunto posterior a la reunión ministerial UE-EE.UU. en materia de justicia y asuntos de interior de 18 de noviembre de 2013 en Washington: «We are therefore, as a matter of urgency, committed to advancing rapidly in the negotiations on a meaningful and comprehensive data protection umbrella agreement in the field of law enforcement. The agreement would act as a basis to facilitate transfers of data in the context of police and judicial cooperation in criminal matters by ensuring a high level of personal data protection for U.S. and EU citizens. We are committed to working to resolve the remaining issues raised by both sides, including judicial redress (a critical issue for the EU). Our aim is to complete the negotiations on the agreement ahead of summer 2014.» (Por consiguiente, estamos decididos, de manera urgente, a avanzar rápidamente en la negociación de un acuerdo marco significativo y completo en materia de protección de datos en el ámbito de la aplicación de la ley. El acuerdo serviría de base para facilitar las transferencias de datos en el contexto de la cooperación policial y judicial en asuntos penales, garantizando un elevado nivel de protección de los datos personales de los ciudadanos de los Estados Unidos y de la UE. Estamos decididos a colaborar para resolver las cuestiones pendientes planteadas por ambas Partes, incluido el recurso judicial (que es un aspecto crucial para la UE). Nuestro objetivo es finalizar la negociación del acuerdo antes del verano de 2014.)

realice en casos claramente definidos, excepcionales y revisables judicialmente. Los Estados Unidos deben comprometerse a este respecto[25].

Un «acuerdo marco» de esta naturaleza debería proporcionar el marco general para garantizar un elevado nivel de protección de los datos personales transferidos a los Estados Unidos a efectos de prevención y lucha contra la delincuencia y el terrorismo. Cando sea necesario, y debido a la naturaleza de los datos transferidos de que se trata, los acuerdos sectoriales deberían establecer disposiciones y garantías adicionales, a semejanza de los Acuerdos PNR y TFTP entre la UE y los Estados Unidos, que establecen condiciones estrictas para la transferencia de datos y las garantías para los ciudadanos de la UE.

3.4. Dar respuesta a las preocupaciones europeas en el proceso de reforma en curso en EE.UU.

El presidente Obama ha anunciado una revisión de las actividades de las autoridades de seguridad nacional estadounidenses, incluido el marco jurídico aplicable. Este proceso en curso ofrece una importante oportunidad de responder a las preocupaciones despertadas en la UE por las recientes revelaciones acerca de los programas de recogida de información de los Estados Unidos. Los cambios más importantes serían la extensión de las garantías de que gozan los ciudadanos y residentes estadounidenses a los ciudadanos de la UE que no residen en los Estados Unidos, el aumento de la transparencia de las actividades de los servicios de información y un mayor refuerzo de la supervisión. Tales cambios restablecerían la confianza en los intercambios de datos entre la UE y los Estados Unidos y fomentarían el uso de los servicios de internet por los europeos.

Por lo que se refiere a la extensión de las garantías ofrecidas a los ciudadanos y residentes estadounidenses a los ciudadanos de la UE, deben revisarse las normas jurídicas en relación con los programas de vigilancia estadounidenses que tratan de modo diferente a los ciudadanos de los Estados Unidos y de la UE, incluso desde la perspectiva de los principios de necesidad y proporcionalidad, teniendo en cuenta la estrecha asociación de seguridad transatlántica basada en valores, derechos y libertades comunes. Ello reduciría la medida en que los europeos se ven afectados por los programas de recogida de información de los Estados Unidos.

Es necesaria una mayor transparencia sobre el marco jurídico de los programas de recogida de información de los Estados Unidos y su interpretación por los tribunales de dicho país, así como sobre la dimensión cuantitativa de tales programas. Los ciudadanos de la UE también se beneficiarían de dichos cambios.

La supervisión de dichos programas podría mejorarse fortaleciendo el papel del «Foreign Intelligence Surveillance Court» (Tribunal de Vigilancia de Inteligencia Exterior) y estableciendo vías de recurso para los particulares. Estos mecanismos podrían reducir el

[25] Véase el fragmento correspondiente del comunicado de prensa conjunto posterior a la reunión ministerial UE-EE.UU. en materia de justicia y asuntos de interior de 18 de noviembre de 2013 en Washington: «We also underline the value of the EU-U.S. Mutual Legal Assistance Agreement. We reiterate our commitment to ensure that it is used broadly and effectively for evidence purposes in criminal proceedings. There were also discussions on the need to clarify that personal data held by private entities in the territory of the other party will not be accessed by law enforcement agencies outside of legally authorized channels. We also agree to review the functioning of the Mutual Legal Assistance Agreement, as contemplated in the Agreement, and to consult each other whenever needed.» (Asimismo destacamos el valor del Acuerdo de Asistencia Judicial Mutua. Reiteramos nuestro compromiso de garantizar que se utiliza en sentido amplio y eficaz con fines de prueba en los procesos penales. También se debatió sobre la necesidad de aclarar que los datos personales conservados por entidades privadas en el territorio de la otra Parte no serán accesibles a los servicios con funciones coercitivas fuera de los canales autorizados legalmente. Del mismo modo, acordamos revisar el funcionamiento del Acuerdo de Asistencia Judicial Mutua, según lo previsto en el Acuerdo, y consultarnos mutuamente siempre que sea necesario.)

tratamiento de los datos personales de los ciudadanos europeos que no son pertinentes con fines de seguridad nacional.

3.5. Fomentar la adopción de normas internacionales de protección de la privacidad

Las cuestiones planteadas por los métodos modernos de protección de datos no se limitan a la transferencia de datos entre la UE y los Estados Unidos. Debe garantizarse también un elevado nivel de protección de los datos personales de todas las personas. Las normas de la UE sobre recogida, tratamiento y transferencia de datos deben promoverse a nivel internacional.

Recientemente, se han propuesto una serie de iniciativas de fomento de la protección de la privacidad, especialmente en internet[26]. La UE debe garantizar que, si se llevan a cabo, tales iniciativas tengan plenamente en cuenta los principios de protección de los derechos fundamentales, la libertad de expresión, los datos personales y la privacidad, establecidos en la legislación de la UE y expuestos en la Estrategia de Ciberseguridad de la UE, y no socaven la libertad, la apertura y la seguridad del ciberespacio. Ello incluye un modelo de gobernanza pluripartito, democrático y eficiente.

Las reformas en curso de la legislación sobre protección de datos a ambos lados del Atlántico también proporcionan a la UE y los Estados Unidos una oportunidad única para establecer una norma internacional. Los intercambios transatlánticos e internacionales de datos resultarían muy beneficiados del reforzamiento del marco jurídico nacional de los Estados Unidos, incluida la aprobación de la «Consumer Privacy Bill of Rights» (Carta de Derechos sobre la Privacidad de los Consumidores) anunciada por el presidente Obama en febrero de 2012 en el marco de un plan completo para mejorar la protección de la privacidad de los consumidores. La existencia de un conjunto de normas de protección de datos rigurosas y oponibles, establecidas tanto en la UE como en los Estados Unidos, constituiría una base sólida para los flujos de datos transfronterizos.

A fin de fomentar las normas internacionales de protección de la privacidad, debe promoverse también la adhesión al Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal («Convenio 108»), que está abierto a países que no son miembros del Consejo de Europa[27]. Las salvaguardias y garantías acordadas en los foros internacionales deberían dar como resultado un nivel elevado de protección compatible con el que se exige en la legislación de la UE.

4. CONCLUSIONES Y RECOMENDACIONES

Las cuestiones señaladas en la presente Comunicación precisan de una actuación de los Estados Unidos, así como de la UE y de sus Estados miembros.

Las preocupaciones acerca de los intercambios de datos a escala transatlántica suponen, ante todo, una llamada de atención a la UE y sus Estados miembros para que avancen con rapidez y ambición en la reforma de la protección de datos. Ponen de manifiesto que es necesario, más que nunca, un marco legislativo sólido, con normas claras y con fuerza ejecutiva también en los casos en que se transfieren datos al extranjero. Por ello, las instituciones de la UE deben seguir trabajando para la aprobación de la reforma de la UE en materia de protección de datos en la primavera de 2014 a más tardar, a fin de garantizar que los datos personales se protejan de manera eficaz y completa.

---

[26] Véase, a este respecto, el proyecto de resolución propuesto a la Asamblea General de las Naciones Unidas por Alemania y Brasil, en el que se hace un llamamiento a la protección de la vida privada tanto en línea como fuera de línea.

[27] Los Estados Unidos ya son Parte en otro Convenio del Consejo de Europa, a saber, el Convenio sobre la Ciberdelincuencia (conocido también con el nombre de «Convenio de Budapest»).

Dada la importancia de los flujos transatlánticos de datos, es esencial que los instrumentos en que se basan esos intercambios se utilicen adecuadamente para afrontar los retos y aprovechar las oportunidades de la era digital y los nuevos desarrollos tecnológicos, como la computación en nube. Los arreglos y acuerdos existentes y futuros deben garantizar la continuidad de un elevado nivel de protección a ambos lados del Atlántico.

Un régimen de puerto seguro sólido redunda en interés de los ciudadanos y las empresas de la UE y de los Estados Unidos. Debería reforzarse mediante un mejor seguimiento y aplicación a corto plazo, y, sobre esa base, mediante una revisión más amplia de su funcionamiento. Son necesarias mejoras para garantizar que se siguen cumpliendo los objetivos iniciales de la Decisión de puerto seguro, a saber, la continuidad de la protección de los datos, la seguridad jurídica y el flujo libre de datos entre la UE y los Estados Unidos.

Estas mejoras deben centrarse en la necesidad de que las autoridades estadounidenses supervisen y controlen mejor el cumplimiento de los principios de puerto seguro por parte de las empresas autocertificadas.

Asimismo, es importante que la excepción por motivos de seguridad nacional prevista en la Decisión de puerto seguro solo se utilice en la medida en que sea estrictamente necesaria y proporcionada.

En el ámbito de la aplicación de la ley, la negociación en curso de un acuerdo marco debería dar como resultado un nivel elevado de protección para los ciudadanos de ambos lados del Atlántico. Tal acuerdo reforzaría la confianza de los europeos en los intercambios de datos entre la Unión Europea y los Estados Unidos y proporcionaría una base para seguir desarrollando la cooperación y la asociación en materia de seguridad entre la Unión Europea y los Estados Unidos. En el contexto de la negociación, convendría contraer compromisos para que los europeos no residentes en los Estados Unidos puedan beneficiarse de las garantías procesales, incluidas las vías de recurso judicial.

Debería conseguirse que las autoridades estadounidenses se comprometieran a garantizar que los datos personales conservados por entidades privadas en la UE no sean directamente accesibles para los servicios con funciones coercitivas estadounidenses al margen de los canales formales de cooperación, como los acuerdos de asistencia jurídica mutua y los acuerdos sectoriales (por ejemplo, el PNR y el TFTP) que autorizan tales transferencias en condiciones estrictas, excepto en casos definidos claramente, excepcionales y revisables judicialmente.

Además, los Estados Unidos deben extender las garantías de que disfrutan los ciudadanos y residentes estadounidenses a los ciudadanos de la UE que no residen en los Estados Unidos, garantizar que sus programas respetan los principios de necesidad y proporcionalidad, y acrecentar la transparencia y supervisión del marco jurídico aplicable a las autoridades estadounidenses competentes en materia de seguridad nacional.

Los ámbitos que se mencionan en la presente Comunicación exigen un compromiso constructivo a ambos lados del Atlántico. Juntos, como socios estratégicos, la UE y los Estados Unidos tienen la capacidad de superar las tensiones actuales de las relaciones transatlánticas y de restablecer la confianza en los flujos de datos entre la Unión Europea y los Estados Unidos. La adopción de compromisos políticos y jurídicos conjuntos en favor de una mayor cooperación en estos ámbitos reforzará las relaciones transatlánticas en general.