

# SUPERVISOR EUROPEO DE PROTECCIÓN DE DATOS

## Resumen ejecutivo del dictamen del Supervisor Europeo de Protección de Datos sobre el proyecto de decisión relativo a la adecuación del escudo protector de la intimidad entre la UE y los EE. UU.

(El texto completo del presente dictamen está disponible en inglés, francés y alemán en el sitio web del SEPD [www.edps.europa.eu](http://www.edps.europa.eu))

(2016/C 257/05)

Los datos fluyen a escala mundial. La UE está vinculada por los Tratados y por la Carta de los Derechos Fundamentales de la Unión Europea, que protegen a todos los ciudadanos en la UE. La UE está obligada a adoptar todas las medidas necesarias para garantizar el respeto del derecho a la privacidad y del derecho a la protección de los datos personales en todas las operaciones de tratamiento, incluidas las transmisiones de información.

Desde que en 2013 se tuvo conocimiento de la existencia de actividades de vigilancia, la UE y los Estados Unidos, socio estratégico de la Unión, han trabajado para definir un nuevo conjunto de normas basado en un sistema de autocertificación para la transmisión de datos personales desde la UE a los EE. UU. con fines comerciales. Al igual que las autoridades nacionales de protección de datos a nivel de la UE, el Supervisor Europeo de Protección de Datos (SEPD) reconoce el valor de un marco jurídico sostenible para las transmisiones de datos con fines comerciales entre la UE y los EE. UU. — que representa la mayor alianza comercial del planeta— en una era en la que los flujos de datos son mundiales, instantáneos e impredecibles. No obstante, dicho marco debe reflejar plenamente los valores comunes democráticos y basados en los derechos individuales; en la UE, estos valores se expresan en el Tratado de Lisboa y en la Carta de los Derechos Fundamentales, mientras que, en el caso de los Estados Unidos, están recogidos en su Constitución.

El proyecto de escudo protector de la intimidad («Privacy Shield») puede representar un paso en la dirección correcta, si bien en su formulación actual no incluye, a juicio del SEPD, todas las medidas adecuadas para proteger los derechos que contempla la UE en relación con la protección de la intimidad individual y los datos personales, así como en lo que respecta al recurso judicial. Si la Comisión Europea desea adoptar una decisión con respecto a su adecuación, será necesario introducir mejoras sustanciales. En particular, la UE debería obtener garantías adicionales en términos de necesidad y proporcionalidad, en lugar de legitimar un acceso rutinario a los datos transmitidos por parte de las autoridades estadounidenses con base en criterios fundamentados jurídicamente en el país receptor, pero no en la UE, como se recoge en los Tratados, la normativa de la UE y las tradiciones constitucionales comunes de los Estados miembros.

Además, en una época de hiperconectividad y redes distribuidas, la autorregulación de las organizaciones privadas y las declaraciones y compromisos de los funcionarios públicos pueden desempeñar un importante papel en el corto plazo. Sin embargo, a más largo plazo pueden no ser suficientes para proteger los derechos y los intereses de los ciudadanos y para satisfacer plenamente las necesidades de un mundo digital globalizado, en el que muchos países cuentan ya con normas relativas a la protección de datos.

En consecuencia, sería deseable alcanzar una solución a largo plazo en el diálogo transatlántico, de manera que la legislación federal vinculante recoja también de forma clara y concisa, como mínimo, los principios fundamentales de los derechos, como sucede con otros países ajenos a la UE que, tras someterse a una evaluación rigurosa, se ha determinado que garantizan un nivel de protección adecuado; lo que el Tribunal de Justicia de la Unión Europea (TJUE), en su sentencia en el asunto Schrems, expresó como «esencialmente equivalente» a las normas aplicables en virtud del derecho de la UE, y que, de conformidad con el Grupo de Trabajo del artículo 29 significa que contiene «la sustancia de los principios fundamentales» de la protección de datos.

El SEPD toma nota con agrado del mayor nivel de transparencia demostrado por las autoridades estadounidenses en cuanto al uso de la excepción a los principios del escudo protector de la intimidad a efectos de ejecución de la legislación, de la seguridad nacional y del interés público.

Sin embargo, aunque la Decisión de puerto seguro de 2000 trataba formalmente el acceso con fines de seguridad nacional como una excepción, la atención que en el proyecto de decisión sobre el escudo protector de la intimidad se dedica al acceso, el filtrado y el análisis de los datos personales transmitidos con fines comerciales por parte de las organizaciones de inteligencia y de los organismos de cumplimiento de la ley indica que tal excepción se ha convertido en la regla. En particular, a partir del proyecto de decisión y de sus anexos, el SEPD toma nota de que, pese a las tendencias recientes, consistentes en abandonar la vigilancia indiscriminada para adoptar enfoques más selectivos, la dimensión de la inteligencia de señales y el volumen de datos transmitidos desde la UE, que podrían ser captados y utilizados una vez transmitidos, en particular durante el tránsito, pueden seguir siendo elevados y, por lo tanto, dignos de reflexión.

Aunque estas prácticas también pueden guardar relación con las actividades de inteligencia en otros países, y si bien el SEPD acoge con satisfacción la transparencia de las autoridades estadounidenses con respecto a esta nueva realidad, el actual proyecto de decisión podría legitimar este tipo de rutina. Por consiguiente, el SEPD alienta a la Comisión Europea a enviar una señal más firme: dadas las obligaciones que emanan del Tratado de Lisboa para la UE, las autoridades

públicas únicamente deberían poder acceder a los datos transmitidos con fines comerciales y utilizarlos, incluso durante su tránsito, en circunstancias excepcionales y solo cuando sea indispensable por motivos específicos relacionados con el interés público.

En relación con las disposiciones relativas a las transmisiones de información con fines comerciales, no debería esperarse que los controladores modifiquen constantemente los modelos de cumplimiento. Y, sin embargo, el proyecto de decisión se ha basado en el marco jurídico actual de la UE, que será sustituido por el Reglamento (UE) 2016/679 (Reglamento general de protección de datos) en mayo de 2018, menos de un año después de la plena aplicación del escudo protector de la intimidad por parte de los controladores. El Reglamento general de protección de datos (RGPD) refuerza las obligaciones de los controladores y crea otras nuevas, que trascienden los nueve principios desarrollados en el escudo protector de la intimidad. Con independencia de los cambios que se introduzcan en la versión definitiva del texto, el SEPD recomienda a la Comisión Europea que lleve a cabo una evaluación exhaustiva de las perspectivas de futuro desde su primer informe, a fin de identificar a tiempo los pasos pertinentes para alcanzar soluciones a más largo plazo para sustituir el escudo protector de la intimidad, en su caso, por marcos jurídicos más sólidos y estables que impulsen las relaciones transatlánticas.

En consecuencia, el SEPD expone a continuación una serie de recomendaciones específicas sobre el escudo protector de la intimidad.

## I. Introducción

El 6 de octubre de 2015, el Tribunal de Justicia de la Unión Europea (en adelante, TJUE) anuló <sup>(1)</sup> la Decisión sobre la adecuación de los principios de puerto seguro <sup>(2)</sup>. El 2 de febrero de 2016, la Comisión Europea alcanzó un acuerdo político con los EE. UU. sobre un nuevo marco para las transmisiones de datos personales, denominado «the EU-U.S. Privacy Shield» (en adelante, el escudo protector de la intimidad). El 29 de febrero, la Comisión Europea hizo público un proyecto de decisión sobre la idoneidad de este nuevo marco (el «proyecto de decisión») <sup>(3)</sup> y sus siete anexos, incluidos los principios del escudo protector de la intimidad y una serie de declaraciones y compromisos por escrito por parte de funcionarios y autoridades estadounidenses. El SEPD recibió el proyecto de decisión el 18 de marzo de este año para que hiciera llegar sus observaciones al respecto.

El SEPD ha manifestado en reiteradas ocasiones su posición <sup>(4)</sup> en lo que respecta a las transmisiones de datos personales entre la UE y los Estados Unidos y ha participado en el dictamen del Grupo de Trabajo del artículo 29 (en adelante, GT29) sobre el proyecto de decisión como miembro de dicho grupo <sup>(5)</sup>. El GT29 ha planteado importantes preocupaciones y ha pedido a la Comisión Europea que identifique soluciones para abordarlas. Los miembros del GT29 esperan que se proporcionen todas las aclaraciones solicitadas en su dictamen <sup>(6)</sup>. El 16 de marzo, 27 organizaciones sin ánimo de lucro plantearon sus críticas al proyecto de decisión en una carta dirigida a las autoridades de la UE y de los EE. UU. <sup>(7)</sup>. El 26 de mayo, el Parlamento Europeo aprobó una resolución sobre los flujos de datos transatlánticos <sup>(8)</sup>, en la que insta a la Comisión a negociar la introducción de mejoras adicionales en el acuerdo sobre el escudo protector de la intimidad con la administración estadounidense en vista de las deficiencias que presenta actualmente el texto <sup>(9)</sup>.

En su condición de asesor independiente de los legisladores de la UE en virtud del Reglamento (CE) n.º 45/2001, el SEPD formula sus recomendaciones a las partes implicadas en el proceso, en particular a la Comisión. Dichas recomendaciones, que pretenden ser pragmáticas y estar adecuadamente fundamentadas, tienen la finalidad de ayudar a la UE a lograr sus objetivos a través de la adopción de medidas adecuadas. Complementan y destacan algunas de las recomendaciones recogidas en el dictamen del GT29, aunque no todas ellas.

<sup>(1)</sup> Asunto C-362/14, Maximilian Schrems c. Comisario europeo encargado de la protección de datos, 6 de octubre de 2015 (en adelante, «Schrems»).

<sup>(2)</sup> Decisión 2000/520/CE de la Comisión, de 26 de julio de 2000, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América (notificada con número de documento C(2000) 2441) (DO L 215, de 25.8.2000, p. 7).

<sup>(3)</sup> Decisión de Ejecución de la Comisión de XXX con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección conferida por el escudo protector de la intimidad UE-EE. UU., disponible (en inglés) en: [http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision\\_en.pdf](http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf)

<sup>(4)</sup> Véase el dictamen del Supervisor Europeo de Protección de Datos respecto a la Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre cómo recuperar la confianza en los flujos de datos entre la UE y los EE. UU. y la Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el funcionamiento del puerto seguro desde la perspectiva de los ciudadanos de la UE y las empresas establecidas en la UE, de 20 de febrero de 2014, así como el escrito procesal presentado por el SEPD en la vista del TJUE en el asunto Schrems, disponible (en inglés) en: [https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Court/2015/15-03-24\\_EDPS\\_Pleading\\_Schrems\\_vs\\_Data\\_Commissioner\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Court/2015/15-03-24_EDPS_Pleading_Schrems_vs_Data_Commissioner_EN.pdf)

<sup>(5)</sup> Grupo de Trabajo del artículo 29 en el dictamen 1/2016 sobre la decisión acerca de la adecuación del escudo protector de la intimidad UE-EE. UU. (GT 238), disponible (en inglés) en: [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf)

<sup>(6)</sup> Véase también el discurso del Comisario de Información del Reino Unido, Christopher Graham, en la conferencia IAPP Europe Data Protection Intensive 2016, celebrada en Londres. El vídeo del discurso está disponible en: <https://iapp.org/news/video/iapp-europe-data-protection-intensive-2016-christopher-graham-keynote/>

<sup>(7)</sup> Carta dirigida al Grupo de Trabajo del artículo 29 y a otras instituciones, firmada por Access Now y otras 26 ONG.

<sup>(8)</sup> Resolución del Parlamento Europeo de 26 de mayo de 2016 sobre los flujos de datos transatlánticos [2016/2727(RSP)].

<sup>(9)</sup> *Idem*, párr. 14.

El proyecto de decisión contiene una serie de mejoras en comparación con la Decisión de puerto seguro, en particular en lo que respecta a los principios aplicables al tratamiento de datos con fines comerciales. En cuanto al acceso por parte de las autoridades públicas a los datos transmitidos bajo el escudo protector de la intimidad, el SEPD también acoge con beneplácito la implicación, por primera vez, del Departamento de Justicia, del Departamento de Estado y de la Oficina del Director de Inteligencia Nacional en las negociaciones. Sin embargo, el progreso realizado en comparación con la Declaración de puerto seguro no es suficiente en sí mismo. La referencia correcta de comparación no es una decisión que había sido invalidada previamente, puesto que la decisión sobre la adecuación debe basarse en el marco jurídico actual de la UE (en particular, la propia Directiva, el artículo 16 del Tratado de Funcionamiento de la Unión Europea y los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea, tal como ha interpretado el TJUE). El artículo 45 del Reglamento general de protección de datos de la UE (RGPD) <sup>(1)</sup> proporcionará nuevos requisitos para las transmisiones de datos, basados en una decisión sobre la adecuación.

El año pasado, el TJUE afirmó que el umbral aplicable a la evaluación de la adecuación es la «equivalencia esencial» y exigió una evaluación estricta basada en este elevado listón <sup>(2)</sup>. La adecuación no obliga a adoptar un marco idéntico al existente en la UE, si bien, en conjunto, el escudo protector de la intimidad y el ordenamiento jurídico estadounidense deberían abarcar la totalidad de los elementos clave del marco vigente en la UE en materia de protección de datos. Esto requiere tanto una evaluación global del ordenamiento jurídico como el examen de los elementos más importantes del marco de protección de datos de la UE <sup>(3)</sup>. El SEPD parte de la hipótesis de que la evaluación debería llevarse a cabo en términos globales, respetando la esencia de dichos elementos. Además, con arreglo al Tratado y a la Carta, será necesario tener en cuenta determinados elementos, como la supervisión independiente y el recurso judicial.

En este sentido, el SEPD es consciente de que muchas organizaciones de ambos lados del Atlántico están esperando el resultado de esta decisión sobre la adecuación. No obstante, las consecuencias de una nueva anulación por parte del TJUE debido a la incertidumbre jurídica de los interesados y a la carga asociada, en particular para las pymes, pueden ser importantes. Además, si el proyecto de decisión es aprobado y posteriormente invalidado por el TJUE, cualquier nuevo acuerdo relativo a la adecuación debería negociarse con arreglo al RGPD. En consecuencia, el SEPD recomienda adoptar un enfoque con visión de futuro, teniendo en cuenta la inminencia de la plena aplicación del RGPD, que tendrá lugar dentro de dos años.

El proyecto de decisión es clave para las relaciones entre la UE y los Estados Unidos, en un momento en que ambos se encuentran inmersos en negociaciones comerciales y de inversión. Asimismo, muchos de los elementos considerados en el dictamen del SEPD resultan pertinentes indirectamente tanto para el escudo protector de la intimidad como para otras herramientas de transmisión de información, como las normas corporativas vinculantes y las cláusulas contractuales tipo. Pero el dictamen también tiene relevancia mundial, dado que numerosos terceros países se guiarán por él en el contexto de la adopción del nuevo marco de la UE sobre protección de datos.

Por consiguiente, el SEPD acogería con agrado una solución general para las transmisiones de datos de la UE a los EE. UU., una solución que debería ser suficientemente sólida e integral. Esto requiere la introducción de importantes mejoras para garantizar que, a largo plazo, se respeten nuestros derechos y libertades fundamentales. Una vez adoptada y tras la primera evaluación de la Comisión Europea, la Comisión deberá ser revisada oportunamente con el fin de identificar las medidas pertinentes para alcanzar soluciones a más largo plazo y sustituir el escudo protector de la intimidad por un marco jurídico más estable y robusto que impulse las relaciones transatlánticas.

Además, a partir del proyecto de decisión y de sus anexos, el SEPD toma nota de que, pese a las tendencias recientes, consistentes en abandonar la vigilancia indiscriminada para adoptar enfoques más selectivos, la dimensión de la inteligencia de señales y el volumen de datos transmitidos desde la UE, que podrían ser captados y utilizados una vez transmitidos, en particular durante el tránsito, pueden seguir siendo elevados y, por lo tanto, dignos de reflexión.

Aunque estas prácticas también pueden guardar relación con las actividades de inteligencia en otros países, y si bien el SEPD acoge con satisfacción la transparencia de las autoridades estadounidenses con respecto a esta nueva realidad, se podría interpretar que el actual proyecto de decisión legitima este tipo de rutina. Este asunto debe someterse a un control democrático público serio. Por consiguiente, el SEPD alienta a la Comisión Europea a enviar una señal más firme: dadas las obligaciones que emanan del Tratado de Lisboa para la UE, las autoridades públicas únicamente deberían poder acceder a los datos transmitidos con fines comerciales y utilizarlos, incluso durante su tránsito, con carácter excepcional y solo cuando sea indispensable por motivos específicos relacionados con el interés público.

Además, el SEPD toma nota de que, al parecer, las declaraciones esenciales para la vida privada de los ciudadanos de la UE únicamente se elaboran con un grado suficiente de detalle en la correspondencia interna que se intercambian las autoridades estadounidenses (por ejemplo, declaraciones relativas a las actividades de inteligencia de señales sobre los

<sup>(1)</sup> Reglamento (UE) 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 estos datos, y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DO L 119, de 4.5.2016, p. 1).

<sup>(2)</sup> *Schrems*, apartados 71, 73, 74 y 96.

<sup>(3)</sup> Este planteamiento ya se consideró en uno de los primeros documentos del GT29 sobre el tema de las transmisiones de datos (GT12: «Transferencias de datos personales a terceros países: aplicación de los artículos 25 y 26 de la Directiva sobre protección de datos de la UE», 24 de julio de 1998).

cables transatlánticos, en su caso) <sup>(1)</sup>. Si bien el SEPD no cuestiona la autoridad de los distinguidos autores de dichas misivas y entiende que, una vez publicadas en el Diario Oficial del Registro Federal, dichas comunicaciones se considerarán «garantías por escrito» sobre las que se realizará la evaluación de la UE, el SEPD toma nota con carácter general de que, por su importancia, algunas de ellas serían merecedoras de un valor jurídico superior.

Además de modificaciones legislativas y acuerdos internacionales <sup>(2)</sup>, cabe explorar otras soluciones de carácter práctico. El presente dictamen aspira a ofrecer orientaciones pragmáticas en ese sentido.

#### IV. Conclusión

El SEPD acoge con satisfacción los esfuerzos demostrados por las partes para encontrar una solución para las transmisiones de datos personales de la UE a los EE. UU. con fines comerciales en el marco de un sistema de autocertificación. Sin embargo, será necesario introducir importantes mejoras para conseguir diseñar un marco sólido y estable a largo plazo.

Hecho en Bruselas, el 30 de mayo de 2016.

Giovanni BUTTARELLI

*Supervisor Europeo de Protección de Datos*

---

<sup>(1)</sup> Véanse, por ejemplo, las aclaraciones recogidas en el anexo VI, apartado 1, letra a), que el PPD28 aplicaría a los datos recabados a través de los cables transatlánticos por la comunidad de inteligencia estadounidense.

<sup>(2)</sup> En la vista del TJUE en el asunto Schrems, el SEPD manifestó que «la única solución eficaz es la negociación de un acuerdo internacional que establezca una protección adecuada contra la vigilancia indiscriminada, incluidas obligaciones relativas a la supervisión, la transparencia, el recurso judicial y los derechos de protección de datos»; escrito procesal del SEPD presentado durante la vista del Tribunal de Justicia de 24 de marzo de 2015 en el asunto C-362/14 (Schrems c. Comisario europeo encargado de la protección de datos).