La Comisión Europea pone en marcha el *Privacy Shield* UE-EE. UU.: más protección para los flujos transatlánticos de datos de carácter personal

Isabela Crespo Vitorique e **Iban Díez López**
Asociados senior *del Área de IP-IT de Gómez-Acebo & Pombo*

El pasado 12 de julio del 2016, la Comisión Europea aprobó el acuerdo conocido como «Privacy Shield entre la Unión Europea y los Estados Unidos», que tiene como objetivo fijar el marco jurídico que regula el flujo de datos entre ambos continentes, protegiendo de forma más efectiva los derechos fundamentales y los datos de los individuos. Este acuerdo establece las bases para que se puedan producir las transferencias transatlánticas de datos personales entre empresas de la Unión Europea y de los Estados Unidos con las mismas garantías que ofrece la normativa europea y recogiendo las carencias que el Tribunal de Justicia de la Unión Europea detectó en su Sentencia de 6 de octubre del 2015, por la que declaraba inválido el antiguo acuerdo de *Safe Harbor*. Asimismo, este acuerdo incluye ciertas garantías y salvaguardas para evitar el tratamiento masivo de datos de ciudadanos europeos por parte de los servicios de inteligencia estadounidenses.

1. El *Privacy Shield* como base para el flujo seguro de datos entre empresas de los Estados Unidos y la Unión Europea. Sustitución del antiguo *Safe Harbor*

Al igual que ocurría con el antiguo sistema de *Safe Harbor*, el *Privacy Shield* se basa en un sistema de autocertificación por adhesión por parte de las empresas de los Estados Unidos a una serie de *principios de privacidad* en relación con el tratamiento de datos personales procedentes de la Unión Europea:

- *Principio de notificación:*

  Las empresas estadounidenses estarán obligadas a informar a los titulares de los datos sobre los aspectos clave en el procesamiento de sus datos de carácter personal (tipos de datos recopilados, propósito del procesamiento de los datos, derechos de acceso a la información y condiciones de transmisión o cesión de dichos datos a un tercero).

- *Principio de elección:*

  Las empresas estadounidenses deberán obtener el consentimiento formal por parte de los ciudadanos antes de ceder sus datos personales sensibles a entidades terceras.

- *Principio de seguridad:*

  Las empresas estadounidenses deberán evaluar los riesgos de seguridad en el tratamiento de la información de carácter personal y deberán implantar medidas de seguridad que mitiguen al máximo dichos riesgos. En el caso de que la entidad subcontrate a un tercero de un servicio determinado, se le deberá exigir un nivel de seguridad equivalente al requerido por la entidad para la protección de la información de carácter personal tratada.

N. de la C.: En las citas literales se ha rectificado en lo posible —sin afectar al sentido— la grafía de ciertos elementos (acentos, mayúsculas, símbolos, abreviaturas, cursivas...) para adecuarlos a las normas tipográficas utilizadas en el resto del texto.

- *Principio de integridad y limitación de propósito:*

  Las empresas estadounidenses deberán garantizar la integridad de los datos personales obtenidos; el titular de los datos sólo deberá ser revelado en los casos en que esto sea imprescindible.

- *Principio de acceso:*

  Las empresas estadounidenses deberán informar a los titulares de los datos sobre el contenido de los datos que obran en su poder y deberá facilitarles el acceso a dichos datos en un plazo de tiempo razonable. Las peticiones de acceso a su información personal podrán ser efectuadas por los ciudadanos en cualquier momento y sin justificación previa.

- *Principio de responsabilidad para transmisiones lícitas:*

  La transmisión de información personal a responsables o encargados de tratamiento de manera lícita sólo deberá hacerse si existe justificación expresa. Además, en caso de llevarse a cabo, dichas transmisiones deberán ser notificadas a los ciudadanos originales, según el principio de notificación comentado anteriormente.

- *Principio de responsabilidad, aplicación y cumplimiento:*

  Las empresas estadounidenses deberán implantar sistemas de verificación del cumplimiento de los principios del *Privacy Shield* y deberán informar de su cumplimiento de manera anual por medio de la renovación de su autocertificación, donde deberán acreditar las acciones que han adoptado para ceñirse a los principios del *Privacy Shield.* En el caso de que las empresas afectadas no demuestren el cumplimiento de dichos requerimientos, saldrán de la lista de empresas adheridas al *Privacy Shield* y estarán sujetas a sanciones económicas.

  Las empresas estadounidenses que decidan voluntariamente adherirse al *Privacy Shield* deberán, en primer lugar, poner en marcha en su organización las medidas necesarias para garantizar que cumplen todos estos principios. Posteriormente, podrán solicitar el certificado de adhesión ante el Departamento de Comercio, quien mantendrá una *lista actualizada de empresas que se hayan adherido al Privacy Shield.* Como explicamos más arriba, anualmente las empresas deberán renovar su certificación de adhesión al *Privacy Shield*.

  El Departamento de Comercio americano deberá garantizar que las compañías que hayan dejado de estar certificadas continúan cumpliendo las obligaciones derivadas de la adhesión al *Privacy Shield* en cuanto al tratamiento de los datos que se hubiesen recibido cuando la empresa aún estaba certificada. El deber de cumplimiento de estas obligaciones permanecerá vigente mientras la empresa siga tratando dichos datos.

  Este acuerdo establece *mecanismos para la aplicación y cumplimiento efectivos* de los principios que componen el *Privacy Shield* por parte de las empresas certificadas*.* Lo ideal es que las reclamaciones de los afectados las resuelva la propia empresa concernida o, en su caso, que ésta ofrezca gratuitamente mecanismos de resolución alternativa de conflictos. Los particulares también podrán dirigirse a sus autoridades nacionales de protección de datos, que colaborarán con el Departamento de Comercio americano para garantizar que se investiguen y resuelvan las reclamaciones de los ciudadanos de la Unión Europea. Si un asunto no se resuelve por un medio u otro, está previsto, en última instancia, un mecanismo de arbitraje.

  Adicionalmente cabe señalar que, hasta la fecha, no hay obligaciones inherentes a empresas españolas vinculadas a las entidades americanas obligadas.

2. Garantías para evitar abusos por el tratamiento masivo de datos de ciudadanos europeos con fines de seguridad nacional

Este acuerdo contiene obligaciones en materia de transparencia y salvaguardas claras para

el acceso de la Administración estadounidense a datos de ciudadanos europeos. Los Estados Unidos han dado a la Unión Europea garantías de que el acceso a los datos de ciudadanos europeos por parte de las autoridades públicas estadounidenses con fines de seguridad estará sujeto a limitaciones, salvaguardas y mecanismos de supervisión claros. También, por primera vez, cualquier ciudadano de la Unión Europea tendrá a su disposición vías de recurso en esta materia. Los Estados Unidos han descartado una vigilancia masiva indiscriminada de los datos personales transferidos hacia ese país en el marco de este acuerdo de *Privacy Shield*. La Oficina del Director de Inteligencia Nacional asume que la recopilación en bloque de datos sólo podrá utilizarse en condiciones específicas predeterminadas y tiene que ser lo más concreta y precisa posible. La Secretaría de Estado, por su parte, ha establecido un mecanismo de recurso para los europeos en el ámbito de la inteligencia nacional mediante la creación de la figura de «Defensor del Pueblo» a estos efectos dentro del Departamento de Estado.

3. Próximos pasos

Este acuerdo será notificado a los Estados miembros y, con ello, entrará en vigor inmediatamente. Por parte de los Estados Unidos, el acuerdo se publicará en el Registro Federal *(Federal Register)*. Una vez que las empresas hayan tenido ocasión de revisar el marco y de actualizar su cumplimiento, podrán certificarse ante el Departamento de Comercio americano a partir del próximo 1 de agosto.

Al mismo tiempo, la Comisión publicará una breve guía para los ciudadanos en la que explicará las vías de recurso disponibles en caso de que un particular considere que sus datos personales se han utilizado sin tener en cuenta las normas de este acuerdo.

A nivel local, cabe señalar que la Agencia Española de Protección de Datos no se ha manifestado en relación con la aprobación final del acuerdo de *Privacy Shield*; habrá que esperar para saber su visión y opinión al respecto.