Transferencia internacional de datos personales: del Safe Harbour al Privacy Shield

Autor/a

Alfonso Ortega Giménez

Profesor Contratado Doctor de Derecho internacional privado. Universidad Miguel Hernández.

REVISTA LEX MERCATORIA.

Doctrina, Praxis, Jurisprudencia y Legislación

RLM nº4 | Año 2017

Artículo nº 12
Páginas 85-90
revistalexmercatoria.umh.es

ISSN 2445-0936

La transferencia internacional de datos personales siempre ha sido un punto muy polémico en el ámbito de la protección de datos a nivel europeo. El 30 de mayo de 2006, la Gran Sala del Tribunal de justicia de la UE dictó una sentencia sobre los asuntos C-317/04 y C-318/04, Parlamento contra consejo y comisión la nulidad de la Decisión 2004/535/CE de la Comisión, de 14 de mayo de 2004, relativa al carácter adecuado de la protección de los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de los Estados Unidos (DO L 235, p. 11) debido a que el tratamiento de datos objeto de la Decisión se excluye de lo estipulado por la Directiva 95/46, y de la Decisión 2004/496/CE del Consejo, de 17 de mayo de 2004, relativa a la celebración de un Acuerdo entre la Comunidad Europea y los Estados Unidos de Améri-

ca sobre el tratamiento y la transferencia de los datos de los expedientes de los pasajeros por las compañías aéreas al Departamento de seguridad nacional, Oficina de aduanas y protección de fronteras, de los Estados Unidos (DO L 183, p. 83, y corrección de errores en DO 2005, L 255, p. 168) debido a que no puede ser adecuado a derecho la celebración de un acuerdo cuyo objeto se encuentra excluido de la directiva mencionada.

En 2013, la Resolución del Parlamento Europeo de 23 de octubre de 2013, sobre la suspensión del acuerdo TFTP a raíz de la vigilancia de la NSA, insta a la Comisión Europea a actuar sobre la posible suspensión del acuerdo SWIFT de transmisión de datos bancaria.

El último tropiezo lo encontramos en 2015 por otra STJUE de la Gran Sala sobre el asunto C-362/14, caso Schrems, el cual anula la 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 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, porque se ha constatado que Estados Unidos no es considerado un tercer país que garantice un nivel de protección adecuada. El puerto seguro era una institución jurídica que permitía a las empresas la transmisión de datos hacia sociedades en EE.UU, cumpliendo una serie de principios Como referidos a la notificación (información a los afectados), opción (posibilidad de oposición de los afectados), transferencia ulterior a terceras empresas, seguridad, integridad de los datos (principios de finalidad y proporcionalidad), derecho de acceso y aplicación (procedimientos para la satisfacción de los derechos de los afectados). Dichos principios son complementados con las “preguntas más frecuentes”,

Las consecuentes anulaciones de transferencias trasnacionales no hacían más que aumentar la inseguridad jurídica, ya que debían regirse por el derecho de los estados, el cual nunca es homogéneo. Se está tramitando, de forma concurrente con el Reglamento, una nueva decisión referida a la transferencia internacional conocida como *Privacy Shield*, que vendrá a sustituir al mecanismo anterior. El nuevo mecanismo viene precedido de la aprobación de un acuerdo llegado con EE.UU sobre la materia. El día 26 de febrero, se publica el borrador de la decisión en el que se destaca:

a) ***Obligaciones estrictas para las empresas y aplicación rigurosa:*** el nuevo sistema será transparente e incluirá mecanismos eficaces de supervisión para velar por que las empresas observen sus obligaciones, con sanciones o exclusión si no lo hacen. Las nuevas normas contemplan también condiciones estrictas para las transferencias ulteriores a otros socios por las empresas participantes en el sistema.

b) ***Salvaguardias claras y obligaciones de transparencia en cuanto al acceso por parte de la administración estadounidense:*** por primera vez, el Gobierno de los Estados Unidos ha dado a la UE garantías por escrito de los servicios del Director de Inteligencia Nacional de que cualquier acceso de las autoridades públicas por motivos de seguridad nacional estará sujeto a limitaciones, salvaguardias y mecanismos de supervisión claros, lo que impedirá un acceso generalizado a los datos personales. El secretario de Estado estadouniden-

se, John Kerry, se ha comprometido a establecer la posibilidad de recurso en el ámbito de la inteligencia para los ciudadanos europeos a través de un mecanismo de mediación dentro del Departamento de Estado, que será independiente de las agencias nacionales de seguridad. El Mediador hará un seguimiento de las denuncias y consultas de particulares y los informará de si se han respetado las leyes pertinentes.

c) ***Protección eficaz de los derechos de los ciudadanos de la UE con varias posibilidades de recurso:*** en caso de disputa, esta tendrá que resolverla la propia empresa en un plazo de 45 días. Habrá un sistema extrajudicial gratuito de resolución de litigios. Los ciudadanos de la UE también podrán dirigirse a sus autoridades nacionales de protección de datos, que colaborarán con la Comisión Federal de Comercio para garantizar que las reclamaciones no resueltas presentadas por los ciudadanos de la UE se investiguen y resuelvan. Si el asunto no se resuelve por un medio u otro, estará previsto, en última instancia, un mecanismo de arbitraje, que garantizará una solución jurídica ejecutable. Además, las empresas se pueden comprometer al cumplimiento con el asesoramiento de las autoridades de protección de datos europeas. Esto es obligatorio para las empresas que manejan datos en materia de recurso humanos.

d) ***Mecanismo de revisión conjunta anual:*** el mecanismo hará un seguimiento del funcionamiento del Escudo de la privacidad, incluidos los compromisos y las garantías asumidos en materia de acceso a los datos con fines policiales y de seguridad nacional. La Comisión Europea y el Departamento de Comercio de los Estados Unidos llevarán a cabo el examen y asociarán al mismo a expertos nacionales de inteligencia de los Estados Unidos y de las autoridades europeas de protección de datos. La Comisión se basará en las demás fuentes de información disponibles, incluidos los informes de transparencia de las empresas sobre el alcance de las solicitudes de acceso por parte de la administración. La Comisión también celebrará una cumbre anual sobre privacidad con las ONG y partes interesadas para debatir las novedades generales en el ámbito del Derecho de los Estados Unidos en materia de privacidad y su efecto en los europeos. Sobre la base del examen anual, la Comisión presentará un informe al Parlamento Europeo y al Consejo.

El siguiente trámite consistió en la audiencia pública ante la Comisión de Libertades Civiles del Parlamento Europeo en el que asistieron tanto comisarios europeos como representantes del Departamento de Comercio estadounidense para explicar las bondades del acuerdo; por contra, Max Schrems consideró que el texto no avanza en las líneas que son deseables y destaca que es un texto que no podrá cumplirse en la práctica.

Posteriormente, el Grupo de Trabajo del artículo 29 (GT29) publicó el dictamen (1/2016) referido al texto de la futura decisión, en el que se destaca negativamente El hecho de que los principios y garantías ofrecidos por el Escudo de Privacidad se hallen expuestos tanto en la decisión de adecuación como en sus anexos hace que la información sea tanto difícil de encontrar como, en ocasiones, incoherente. Esto contribuye a una falta global de claridad en relación con el nuevo marco y dificulta la accesibilidad a los interesados, las organizaciones y las autoridades de protección

de datos. De modo similar, falta claridad en el lenguaje utilizado.

Destaca también que deberá revisar el acuerdo logrado una vez haya entrado en vigor el Reglamento Europeo de Protección de Datos con el fin de ser acogido más adecuadamente en el nuevo marco jurídico relativo a la materia.

El principio de retención de datos no se menciona expresamente y no se puede inferir del actual enunciado del Principio de Integridad de Datos y Limitación de la Finalidad. Además, no se hace mención a la protección que debe prestarse frente a las decisiones individuales automatizadas basadas exclusivamente en tratamientos automáticos. La aplicación del principio de limitación de finalidad al tratamiento de datos es también confusa.

Sugiere que la UE y EEUU deberían acordar definiciones más claras con las que elaborar un glosario de términos incorporado a la sección de Preguntas Frecuentes del Escudo de Privacidad. Puesto que el Escudo de Privacidad se usará también para transferir datos fuera de EE. UU. el GT29 insiste en que las transferencias ulteriores desde una entidad del Escudo de Privacidad a destinatarios de un país tercero debe proporcionar el mismo nivel de protección en todos los aspectos definidos en el Escudo (incluida la seguridad nacional) y no debe llevar a que se rebajen o se sorteen los principios de protección de datos de la UE. En caso de preverse una transferencia ulterior a un país tercero bajo el Escudo de Privacidad, todas las organizaciones del Escudo de Privacidad deben tener la obligación de evaluar cualquier requisito obligatorio de la legislación nacional del país tercero aplicable al importador de los datos antes de la transferencia. En general, el GT29 concluye que el marco para las transferencias ulteriores de datos personales de la UE es insuficiente, en especial en lo relativo a su alcance, la limitación de su finalidad y las garantías aplicadas a las transferencias a Agentes.

Respecto a la línea cuasi invisible entre seguridad nacional y privacidad, el GT29 recuerda su postura, mantenida desde hace tiempo, de que la vigilancia masiva e indiscriminada de las personas nunca puede considerarse proporcionada y estrictamente necesaria en una sociedad democrática, tal como se requiere de acuerdo con la protección ofrecida por los derechos fundamentales aplicables. Es crucial además que exista una supervisión global de todos los programas de vigilancia.

El dictamen termina destacándolo como un proyecto más garantista que el puerto seguro, pero insta a la Comisión a disipar sus dudas mediante la aplicación de estas recomendaciones.

El 26 de mayo, el Parlamento Europeo emitió una resolución (2016/2727(RSP)) donde aplaudía las reformas realizadas respecto al puerto seguro pero, en la línea del dictamen del GT29, critica que 1) el Defensor del Pueblo estadounidense no sea lo suficientemente independiente; 2) la recolección de datos en bloque no cumpla con los criterios de necesidad y proporcionalidad; 3) la complejidad del recurso. El dictamen insta a hacer más accesible el recurso, a que revisen periódicamente el *privacy shield* y a adoptar las recomendaciones del GT29.

El borrador fue modificado en su versión final aprobada el 8 de julio por el comité del artículo 31 añadiendo mayores garantías contra la recogida masiva de datos y sumando mayor transparencia al papel del Defensor del Pueblo estadounidense. Tal versión final ha

recibido el visto bueno de DIGITALEUROPE, la asociación que aglutina a los gigantes tecnológicos y demás empresas que manejan grandes cantidades de datos.

El texto ahora está pendiente de la aprobación de la Comisión Europea, que se espera que sea durante ls segunda semana de julio.

En el Reglamento, se prevé la posibilidad de transmitir datos personales a terceros estados con un nivel de protección adecuado una vez se haya adoptado una decisión por parte de la Comisión.

Para evaluar el nivel de protección, se tendrán en cuenta los siguientes aspectos.

a) El Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, la legislación pertinente, tanto general como sectorial, incluida la relativa a la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales, así como la aplicación de dicha legislación, las normas de protección de datos, las normas profesionales y las medidas de seguridad, incluidas las normas sobre transferencias ulteriores de datos personales a otro tercer país u organización internacional, la jurisprudencia, y el reconocimiento a los interesados cuyos datos personales estén siendo transferidos de derechos efectivos y exigibles y de recursos administrativos y acciones judiciales que sean efectivos;

b) La existencia y el funcionamiento efectivo de una o varias autoridades de control independientes en el tercer país o a las cuales esté sujeta una organización internacional, con la responsabilidad de garantizar y hacer cumplir las normas en materia de protección de datos, incluidos poderes de ejecución adecuados, de asistir y asesorar a los interesados en el ejercicio de sus derechos, y de cooperar con las autoridades de control de la Unión y de los Estados miembros, y

c) Los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales.

d) Los compromisos internacionales asumidos por el tercer país u organización internacional de que se trate, u otras obligaciones derivadas de acuerdos o instrumentos jurídicamente vinculantes, así como de su participación en sistemas multilaterales o regionales, en particular en relación con la protección de los datos personales.

Se prevé que la decisión se revise cada cuatro años con el objetivo de controlar si ese tercer estado sigue cumpliendo con tales condiciones. Si se observa que ya no se cumple tal nivel, la Comisión derogará, suspenderá o modificará el acuerdo. Se entablarán conversaciones con ese estado para poner remedio a la situación anterior. Se permite también la transferencia a terceros aun no existiendo una decisión, pero habiendo aportado las garantías suficientes, como la adopción de instrumentos vinculantes.

No es el único acuerdo de transferencia internacional con EE.UU , aparte del acuerdo SWIFT, la Unión mantiene acuerdos sobre utilización y transferencia de los registros de

nombres de pasajeros y el muy reciente acuerdo para la transferencia de datos personales para la lucha antiterrorista y la cooperación policial, además de mantener acuerdos similares con Canadá y Australia.

Debemos incluir también la Directiva (UE) 2016/681 del Parlamento Europeo Y del Consejo de 27 de abril de 2016 relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave que pretende armonizar la legislación de todos los Estados miembros a la hora de establecer medidas de registro y protección de forma conjunta, transferencias internacionales, cooperación entre los Estados, obligaciones a las compañías aéreas y la creación de la Unidad Informática de pasajeros.