Relaciones asimétricas

POR **JOSÉ LUIS RODRÍGUEZ ÁLVAREZ**

«La Unión Europea y Estados Unidos son líderes mundiales protegiendo las libertades individuales, incluida la privacidad, mientras que, al mismo tiempo, fomentar la innovación y el comercio es algo crítico para la economía mundial, sobre todo, en el momento actual. Una cooperación transatlántica más sólida en el ámbito de la protección de datos mejorará la confianza del consumidor y promocionará el crecimiento de la economía de Internet global y el mercado común transatlántico digital en desarrollo. […] Es un momento determinante para la protección de datos personal a nivel global y la política de privacidad y para alcanzar una mayor interoperabilidad en nuestros sistemas a un nivel de protección más elevado».

Estas frases, procedentes del comunicado conjunto final de la *Conferencia sobre protección de datos* celebrada en marzo de 2012 con participación de representantes de la Unión Europea y Estados Unidos[1] recogen, aparte de una visión positiva y esperanzada de la realidad que el tiempo parece haber desmentido, algunos de los elementos clave de las relaciones entre Europa y los EEUU en el terreno de la protección de datos.

Ciertamente, ambas regiones comparten valores, intereses económicos y niveles de desarrollo tecnológico. Y ambas regiones se han visto afectadas de forma similar por fenómenos como el de la violencia del terrorismo internacional. La forma en que esos elementos se concretan hace, sin embargo, que las relaciones en materia de protección de datos puedan calificarse, de manera muy sintética, de asimétricas.

Diferencia de criterios

Es sobradamente conocido que mientras que en la UE se considera la protección de datos como un derecho fundamental, al otro lado del Atlántico las garantías para la información personal de los ciudadanos se abordan básicamente como un componente más de las relaciones entre empresas y consumidores. Aunque sin duda eso no impide que en EEUU existan vías para defender la privacidad, lo cierto es que no puede concluirse directamente que la protección de los datos personales tenga un mismo contenido en las dos regiones.

En el ámbito del desarrollo económico, hay que admitir que son sin duda más numerosas las empresas norteamericanas que operan en la UE que las europeas que lo hacen en EEUU. Esa situación es especialmente relevante cuando hablamos de empresas que operan en el ámbito de las Tecnologías de la Información y la Comunicación (TIC) y, más específicamente, en el

Fundación Telefónica

mundo de Internet. Es casi una obviedad reconocer que los gigantes de Internet son, con algunas señaladas excepciones europeas y del área del Pacífico, norteamericanos. De esta realidad se deriva, como consecuencia inmediata, que los datos de ciudadanos europeos tengan muchas probabilidades de ser tratados por empresas americanas y también de ser exportados a EEUU por esas u otras empresas.

Las respuestas que hasta ahora ha dado el derecho europeo a las posibles diferencias en el nivel de protección no han sido, no son aún, todo lo eficaces que sería de desear. Por un lado, los criterios de aplicabilidad de la legislación europea, o más exactamente de las legislaciones nacionales que aplican en cada Estado miembro la legislación europea, la Directiva 95/46, están diseñados en torno a unos presupuestos de presencia territorial propios de la época en que la Directiva fue redactada. Pero actualmente no es necesario tener una sucursal o una filial en un país para dirigirse a sus ciudadanos y ofrecerles bienes o servicios o para acceder a sus datos personales. De ahí que en el mundo de Internet, donde los principales protagonistas son esas grandes corporaciones norteamericanas, resulten muy frecuentes los intentos de eludir la normativa europea de protección de datos alegando que no se cuenta con ningún establecimiento o que no se utilizan medios de tratamiento en la UE.

Para las transferencias de datos a EEUU, la solución ha pasado por el denominado *Safe Harbour* (Puerto Seguro), que se presenta como un modelo de declaración de adecuación sui géneris. En virtud del mismo, se considera que las empresas americanas que cumplan una serie de principios de protección de datos adoptados por el Departamento de Comercio de EEUU ofrecen un nivel de protección adecuado[2].

El Puerto Seguro ha sido desde su puesta en funcionamiento motivo de preocupación para las autoridades de protección de datos europeas[3]. Son varios los aspectos que generan dudas sobre el funcionamiento del sistema, por motivos que tienen que ver, entre otras cosas, con su propia naturaleza como esquema basado en la autocertificación, con la poca claridad de algunas de sus condiciones o con la relativa debilidad de los mecanismos de supervisión del cumplimiento por parte de las empresas de los requisitos del *Safe Harbour*[4].

Con todo, y a pesar de sus limitaciones y de las críticas de que ha sido objeto, el *Safe Harbour* es actualmente el principal instrumento que posibilita las transferencias de datos de la UE a EEUU y el número de las empresas acogidas a él ha crecido hasta alcanzar las más de 3.000, entre las que se incluyen grandes multinacionales del sector de las TIC.

EEUU y la recogida de información en áreas sensibles

Las anteriores consideraciones se refieren a los intercambios vinculados a la actividad empresarial, pero no cabe olvidar que los ataques terroristas de septiembre de 2001 tuvieron como efecto el refuerzo de las políticas de seguridad y de lucha contra el terrorismo de EEUU. Ese refuerzo se ha traducido en una extensión e intensificación sin precedentes de los programas dirigidos a obtener información en áreas consideradas sensibles, lo que, a su vez, ha vuelto a poner a prueba la compatibilidad de los sistemas de protección americano y europeo, ya que estos programas, adoptados y gestionados por autoridades públicas estadounidenses, imponen la recogida y tratamiento de datos de -entre otros- ciudadanos

Fundación Telefónica
Telefónica

europeos.

Dos son los principales programas de este tipo: por un lado, el de recogida de datos de pasajeros en vuelo hacia o desde EEUU (el conocido como PNR), aunque también cabría incluir aquí la recogida de los datos API (*Advanced Passenger Information*); por otro, el de tratamiento de los datos de mensajería electrónica sobre transacciones financieras, conocido como SWIFT -según el nombre de la empresa que presta estos servicios- o, más formalmente, como *Terrorist Financing Tracking Program* (TFTP).

Estos tratamientos han sido desde su inicio, y como ya sucediera con el caso del Puerto Seguro, valorados con prevención por parte de las autoridades de protección de datos europeas[5]. Aun cuando también en Europa se han adoptado medidas similares en el marco de la lucha contra el terrorismo y la delincuencia organizada a gran escala, y asumiendo que también las autoridades europeas tienen acceso a los resultados obtenidos del análisis de esta información que puedan resultarles relevantes, no cabe ignorar que en ambos casos la decisión fue adoptada unilateralmente por parte de las autoridades americanas y ha sido solo con posterioridad cuando desde la UE se ha conseguido llegar a acuerdos que permiten que estos tratamientos de información se produzcan en un marco de garantías[6].

Una novedad relevante en este enfoque la constituyen las negociaciones actualmente en curso para concluir un acuerdo ‘paraguas’ o general entre EEUU y la UE en materia de intercambio de información en el ámbito policial y judicial, que debería proporcionar un marco estable al que referir futuros acuerdos sectoriales.

¿Cómo recobrar la confianza?

Este estado de cosas es al que hacía referencia el comunicado conjunto con el que se abría este artículo. EEUU y la UE están necesariamente obligados a entenderse y, aunque existen puntos de fricción en el terreno de la protección de datos, los desarrollos en los respectivos marcos de privacidad que se anunciaban a principios de 2012 permitían vislumbrar la adopción de medidas de diversa naturaleza que contribuyeran a incrementar la compatibilidad de ambos regímenes y, por tanto, a minimizar el alcance de algunos de esos problemas.

Sin embargo, la revelación en junio de este año de la existencia de programas de vigilancia que suponían el acceso por parte de agencias de inteligencia norteamericanas a cantidades masivas de informaciones de ciudadanos europeos al margen de los acuerdos y garantías existentes ha dado lugar a un replanteamiento de toda la situación. Los principales interrogantes que se plantean son, lógicamente, los relativos a la legalidad y legitimidad de estos accesos, pero los programas revelados cuestionan también la propia utilidad de los mecanismos de garantía actualmente vigentes, si todos ellos pueden ser circunvalados sin aparente dificultad y, como consecuencia de ello, se han agravado notablemente las dudas y las preocupaciones preexistentes.

En la elaboración de la respuesta europea desde la perspectiva de la protección de datos se han tratado paralelamente todas estas dimensiones, y los resultados se han empezado a conocer muy recientemente, de la mano de varios documentos que ha publicado la Comisión

BY NC ND

Europea. El principal de ellos es la *Communication from the Commission to the European Parliament and the Council-Rebuilding Trust in EU-US Data Flows*, cuya versión definitiva todavía no se ha hecho pública en el momento de escribir estas líneas[7].

En la Comunicación, y después de pasar revista a los diversos instrumentos en los que se basan las relaciones EEUU-UE en el terreno de la protección de datos, la Comisión identifica seis áreas en las que debe actuarse para, como señala el título, reconstruir la confianza que los programas de vigilancia han dañado.

Las condiciones de la UE. La primera es la rápida adopción de la reforma del marco europeo de protección de datos. Aunque la Comisión apunta en este caso al establecimiento de reglas claras que puedan ser aplicables también en los casos en que los datos sean transferidos y tratados fuera de la Unión, hay otras disposiciones que pueden ser igualmente importantes. Una es la que tiene que ver con el ámbito de aplicación de la legislación europea. La propuesta de Reglamento General de Protección de Datos prevé que será aplicable para empresas que no estén establecidas en la Unión, pero que traten datos de residentes en ella en el contexto de oferta de bienes o servicios o en el de seguimientos de su actividad. Además, y específicamente en el contexto del acceso a datos en el ámbito policial y judicial, puede tener un especial impacto la disposición incorporada por la Comisión LIBE del Parlamento Europeo respecto a transferencias o cesiones derivadas de órdenes judiciales o administrativas y no autorizadas por el derecho de la Unión[8].

En segundo lugar, la Comisión hace una serie de recomendaciones encaminadas a ‘hacer el Puerto Seguro más seguro’. Esas recomendaciones se plantean después del análisis contenido en otro documento, también hecho público por la Comisión, en el que se confirman algunas de las debilidades del sistema que venían siendo criticadas desde su implantación[9]. Entre los puntos que requieren revisión se encuentra la transparencia del sistema, los mecanismos de supervisión o el acceso de los ciudadanos europeos a mecanismos de reparación.

En tercer lugar, la Comisión propone reforzar las garantías de protección de datos en el área de policía y seguridad, manifestando la necesidad de que finalicen rápidamente las negociaciones del acuerdo ‘paraguas’ actualmente en curso, con el objetivo de conseguir un mismo nivel de protección para los ciudadanos en ambos lados del Atlántico. También, y en cuarto lugar, la Comisión demanda que los accesos a información en los ámbitos policial y judicial se produzcan en el seno de los acuerdos de Asistencia Jurídica Mutua y sectoriales existentes, tales como el PNR o SWIFT. Finalmente, se señala que las peticiones de datos directas a las compañías debieran ser solo posibles en situaciones claramente definidas, excepcionales y revisables judicialmente.

Conclusiones

No cabe sino coincidir con los planteamientos de la Comisión, en la medida en que abordan directamente tanto los elementos de asimetría tradicionales como problemas conocidos más recientemente. Sin embargo, no puede evitarse un razonable grado de escepticismo acerca de la positiva conclusión de todas estas iniciativas. De ellas, tan solo la primera depende exclusivamente de las instituciones de la Unión; en los demás casos, el resultado ha de

Fundación Telefónica
Telefónica

proceder de una negociación bilateral, cuando no de decisiones tomadas por las autoridades estadounidenses.

Es, por tanto, imprescindible que las respuestas técnicas vayan acompañadas del compromiso político adecuado para dotar a las relaciones trasatlánticas de unos mayores niveles de equilibrio en materia de protección de datos que contribuyan a lograr la recuperación de la confianza a la que se alude en la Comunicación de la Comisión, tan necesaria en el contexto actual.

Notas

[1] *EU Conference: Privacy and Protection of Personal Data. 19 March 2012, Washington/Brussels – EU-US joint statement on data protection by European Commission Vice-President Viviane Reding and U S Secretary of Commerce John Bryson*.

[2] Decisión de la Comisión 520/2000/CE de 26 de Julio de 2000 sobre la adecuación de la protección ofrecida por los 'Principios de Privacidad del Safe Harbour' y las 'Preguntas Frecuentes relacionadas' adoptados por el Departamento de Comercio de EEUU (Véase: DOCE 215, de 28 de agosto de 2000, p. 7).

[3] Dictamen 4/2000 sobre el nivel de protección que proporcionan los Principios de Puerto Seguro, aprobado el 16 de mayo de 2000.

[4] Un análisis más extenso de estos problemas puede verse en la introducción de la *Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU* [versión no definitiva, en línea]. Disponible en: *http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf*

[5] Ver, a título ilustrativo, las primeras opiniones del Grupo del Artículo 29, a las que han seguido otras varias, en particular en lo relativo a datos PNR: Dictamen 6/2002 relativo a la transmisión de listas de pasajeros y otros datos de compañías aéreas a los Estados Unidos (aprobado el 24 de octubre de 2002) y Dictamen 4/2003 relativo al nivel de protección garantizado en los EEUU para la transferencia de datos de pasajeros (aprobado el 13 de junio de 2003). También el Dictamen 10/2006 sobre el tratamiento de datos personales por parte de la Sociedad de Telecomunicaciones Financieras Interbancarias Mundiales (*Worldwide Interbank Financial Telecommunication*, SWIFT), adoptado el 22 de noviembre de 2006.

[6] La versión más actual de estos programas se encuentra en los anexos a la Decisión del Consejo 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 (2012/472/UE) y a la 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 (2010/412/UE).

Fundación Telefónica

[7] Una versión provisional puede encontrarse en *http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf*

[8] Art. 43.a del texto aprobado por la Comisión LIBE.

[9] Una versión no definitiva de este documento puede encontrarse en: *http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf*

Fundación Telefónica