

# Restaurar la confianza al otro lado del Atlántico

POR **PETER HUSTINX**

La reciente oleada de revelaciones sobre la vigilancia masiva en Internet por parte de Estados Unidos y otros servicios de seguridad ha causado conmoción en todo el mundo y, a su vez, ha supuesto un grave problema a distintos niveles entre la Unión Europea (UE) y Estados Unidos. Ahora, no solo nos hemos enterado de la vigilancia excesiva, exhaustiva y estructural a la que están sometidos todos los ciudadanos en sus quehaceres diarios, sino también de que dicha vigilancia masiva está accediendo a una infraestructura de servicios gratuitos, a menudo dominados por empresas estadounidenses, donde los datos personales de los ciudadanos se controlan continuamente y se transforman en tremendas ganancias publicitarias a través de Internet. Esta infraestructura se ha ido desarrollando gradualmente a lo largo de una década, con cierto y obvio apoyo popular pero con muy poca conciencia pública de las consecuencias que ahora se han hecho visibles. Por otra parte, y de manera importante, también hay una preocupante falta de equilibrio entre los marcos jurídicos aplicables a ambos lados del Atlántico.

La Comisión Europea ha presentado recientemente un plan de acción para recuperar la confianza en los flujos de datos[1] entre la UE y EEUU. Este plan de acción también insta al gobierno estadounidense a contribuir a la restauración de dicha confianza y salvar la brecha actual. Sin embargo, es importante ser conscientes de que los problemas que han surgido tienen raíces muy arraigadas en la historia y la cultura jurídica y que abordarlos será un proceso a largo plazo. En cualquier caso, lo mejor es tratar el asunto del ‘espionaje excesivo’ de manera independiente respecto a otras cuestiones más estructurales, aunque debemos ser conscientes de las conexiones existentes entre ambos aspectos.

## Aspectos comunes y principales diferencias

No obstante, entre la UE y EEUU también existen puntos en común. Las primeras ideas sobre protección de datos personales surgieron en ambos lugares al mismo tiempo, al comienzo de la década de 1970. De hecho, los principios establecidos en el Convenio de Protección de Datos del Consejo de Europa (1981) se basaban en los Principios[2] de Información Justa estadounidenses, que también inspiraron las Directrices de Privacidad de la OCDE (1980).

Sin embargo, la evolución posterior tomó rumbos diferentes: mientras que EEUU, aparte de

algunas normas específicas, se centró especialmente en la autorregulación, la UE siguió invirtiendo en una estructura de leyes nacionales, en el marco de la Directiva 95/46/CE. Esto finalmente llevó al reconocimiento del derecho a la protección de los datos personales como un derecho fundamental independiente, en el artículo 8 de la Carta de los Derechos Fundamentales, que se hizo vinculante en el Tratado de Lisboa a finales de 2009.

Pero tras esta diferencia en la infraestructura jurídica, se encuentra una importante diferencia constitucional: la Cuarta Enmienda de la Constitución estadounidense -la prohibición de registros e investigaciones irrazonables[3]- tiene un alcance mucho más limitado que el derecho al respeto de la vida privada, tal como se establece en el artículo 7 de la Carta de la UE[4]. Como resultado, la Cuarta Enmienda solo se aplica al contenido y no a otros datos en las comunicaciones -como la persona que llama, la hora y la ubicación-; y en principio, solo protege a los ciudadanos estadounidenses. Además, la información confiada a un proveedor de servicios ya no cuenta con su protección, mientras que el punto de partida en la legislación de la UE sigue residiendo en la confidencialidad de las comunicaciones.

A lo largo de los años, se han encontrado soluciones creativas para reducir la brecha entre la legislación de la UE y la autorregulación estadounidense. Un buen ejemplo es la decisión Puerto Seguro[5], que permite la transferencia de datos de la UE a las empresas estadounidenses que hayan empezado a cumplir con los Principios de Puerto Seguro, sujetos a la jurisdicción de la Comisión Federal de Comercio estadounidense, bajo la Ley de Comercio Justo de Estados Unidos. Aunque de momento más de 3.000 empresas se han sumado al acuerdo, siguen existiendo algunos problemas fundamentales y la Comisión[6] ha identificado 13 puntos de mejora y anunciado una revisión a fondo hacia el verano de 2014.

## El marco jurídico de la UE, en proceso de revisión

Mientras tanto, la UE ha invertido mucha energía en una revisión completa de su marco jurídico existente en protección de datos, con el fin de hacerlo más sólido y eficaz, dados los retos que plantean las nuevas tecnologías y la globalización[7]. Esto supondrá unos derechos más consolidados para los titulares de los datos, mayores responsabilidades para los que controlan la información y una supervisión más estricta y el cumplimiento por parte de autoridades independientes. La propuesta de una Regulación de Protección de Datos General[8] -vinculante directamente en todos los Estados miembros- garantizará una mayor consistencia de las normas y prácticas jurídicas en toda la UE. Un marco sólido, con normas claras que sean aplicables también cuando se transfieran datos al extranjero, es ahora -más que nunca- una necesidad.

Un aspecto importante de esta propuesta es que se aplicará a todas las empresas activas en el mercado europeo independientemente de dónde estén operando. Asimismo, el nuevo marco también se aplicará a las empresas establecidas en EEUU o en terceros países, que no estén sujetas a regulaciones similares en su propio país. Probablemente, esto también incluya a operadores conocidos en Internet que puedan haber estado sometidos a vigilancia masiva, mientras atendían a consumidores de la UE. Las nuevas normas ofrecerán un instrumento contra las prácticas indebidas de las empresas, actualmente implicadas en el seguimiento sistemático y la explotación del comportamiento del consumidor. El vasto

tamaño del mercado europeo contribuirá a hacer de esto una opción realista.

Las nuevas normas también podrían proporcionar un mecanismo de regulación[9] para tratar la posibilidad de un conflicto de legislación (inter)nacional, donde las jurisdicciones tengan opiniones contrarias sobre sus intereses públicos. El principio básico debería ser que todos los flujos de datos deben seguir la legislación de la UE, a menos que un acuerdo internacional vinculante disponga lo contrario o que una autoridad judicial o de supervisión conceda una exención. Tal mecanismo podría ser útil en distintas situaciones, incluyendo aquellas que ahora posiblemente se vean afectadas por una vigilancia masiva.

## El plan de acción de la Comisión Europea

En este contexto, es relevante que el plan de acción presentado recientemente por la Comisión Europea también mantenga iniciativas en el contexto de acuerdos internacionales con EEUU[10]. Además de la disposición de Puerto Seguro, sobre la que ya hemos hablado brevemente, la Comisión pretende reforzar las garantías de protección de datos en el ámbito del cumplimiento de la ley. Esto implica la celebración de un acuerdo para la transferencia de datos en el contexto de la cooperación policial y judicial, con un alto nivel de protección a los ciudadanos a ambos lados del Atlántico. Esto también significa que los ciudadanos de la UE no residentes en EEUU deberían beneficiarse de los mecanismos de enmiendas judiciales. La transferencia de datos para propósitos del cumplimiento de la ley debería utilizar canales oficiales. Pedir datos directamente a las empresas de la UE solo debería ser posible en situaciones claramente definidas, excepcionales y revisables judicialmente.

La Comisión Europea también insistió en que las preocupaciones europeas deberían ser tratadas en el continuo proceso de reforma estadounidense. Esto se refiere a la revisión de las actividades de las autoridades de seguridad nacional de EEUU, incluyendo el marco jurídico aplicable, anunciado por el presidente Obama. Los cambios más importantes previstos por la Comisión serían: ampliar las garantías disponibles para los ciudadanos estadounidenses y los residentes, los ciudadanos de la UE que no residan en EEUU, aumentar la transparencia de las actividades de inteligencia y reforzar la supervisión de estas actividades. La necesidad y la proporcionalidad de los programas actuales de vigilancia también deberían considerarse cuidadosamente.

La Comisión Europea también mencionó la creciente necesidad de estándares de privacidad internacionales, especialmente en Internet. En este contexto, se refirió a varias iniciativas recientes, como el proyecto de resolución para la Asamblea General de la ONU propuesto por Alemania y Brasil, basado en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (1966) y que exigía protección de la privacidad en línea y también fuera de ella.

Los intercambios de datos a lo largo del Atlántico y más allá también, se beneficiarían enormemente del fortalecimiento del marco jurídico interno estadounidense, incluida la aprobación de la Declaración de Derechos de la Privacidad del Consumidor, anunciada por el presidente Obama en febrero de 2012 como parte de un completo anteproyecto para mejorar la protección de la privacidad[11] de los consumidores. La existencia de una regulación sólida y aplicable en la protección de datos, con el amparo de la UE y EEUU, proporcionaría,

efectivamente, una base más estable para los flujos de datos transfronterizos.

Por último, no se debería ignorar que los Estados miembros de la UE pueden haber desempeñado o todavía pueden estar desempeñando un papel importante en el tema de la vigilancia masiva. El hecho de que la seguridad nacional sea responsabilidad exclusiva[12] de cada Estado miembro no es, en ningún caso, una buena razón para evitar que se hagan las preguntas correctas y se tomen las medidas adecuadas, a la mayor brevedad posible y en los niveles apropiados.

*Traducción: Belén Moser-Rothschild Criado*

## Notas

[1] Comunicación de la Comisión al Parlamento Europeo y al Consejo, *Rebuilding Trust in EU-US Data Flows*, 27 de noviembre de 2013, COM(2013) 846 final.

[2] Departamento de Sanidad, Educación y Bienestar de Estados Unidos, *Report of the Secretary's Advisory Committee on Automated Personal Data Systems: Records, Computers and the Rights of Citizens* (Washington DC, 1973).

[3] IV Enmienda a la Constitución estadounidense: «El derecho de los habitantes de que sus personas, domicilios, papeles y efectos se hallen a salvo de pesquisas y aprehensiones arbitrarias, será inviolable, y no se expedirán al efecto mandamientos que no se apoyen en un motivo verosímil, estén corroborados mediante juramento o protesta y describan con particularidad el lugar que deba ser registrado y las personas o cosas que han de ser detenidas o embargadas».

[4] Artículo 7 de la Carta: «Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de sus comunicaciones».

[5] Decisión de la Comisión 2000/520/EC del 26 de Julio de 2000 conforme a la Directiva 95/46/EC del Parlamento Europeo y el Consejo sobre la adecuación de la protección ofrecida por los Principios de Privacidad de Puerto Seguro y las preguntas relacionadas más frecuentes emitidas por el Departamento de Comercio estadounidense, OJ L 215, 25.8.2000, p.7.

[6] Comunicación de la Comisión al Parlamento Europeo y al Consejo, *Rebuilding Trust in EU-US Data Flows*, 27 de noviembre de 2013, COM(2013) 846 final.

[7] Ver el Paquete de Reformas presentado por la Comisión en enero de 2012.

[8] Comisión Europea, Propuesta para una Regulación del Parlamento Europeo y del Consejo sobre la protección de los individuos respecto al procesamiento de datos personales y el libre movimiento de dichos datos (Regulación General de Protección de Datos), COM(2012) 11 final.

[9] Ver las enmiendas adoptadas por la Comisión del Parlamento Europeo en Libertades Civiles, Justicia y Asuntos de Interior (LIBE) el 21 de octubre de 2013.

[10] Véase: Comunicación de la Comisión al Parlamento Europeo y al Consejo, *Rebuilding Trust in EU-US Data Flows*, 27 de noviembre de 2013, COM(2013) 846 final.

[11] Véase: *Consumer Data Privacy in a Networked World: a framework for protecting privacy and promoting innovation in the global digital economy*, Febrero de 2012, Washington DC.

[12] Véase el artículo 4(2) del Tratado de la Unión Europea (TUE).

