COMISIÓN
EUROPEA

Bruselas, 29.2.2016
COM(2016) 117 final

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO

Los flujos transatlánticos de datos: recuperar la confianza instaurando estrictas salvaguardias

1. Introducción: la importancia de los intercambios de datos personales en la relación entre la Unión Europea y los Estados Unidos

La existencia de una sólida colaboración transatlántica entre la Unión Europea y los Estados Unidos sigue siendo hoy tan vital como siempre. Compartimos valores, tenemos objetivos políticos y económicos comunes y cooperamos codo con codo en la lucha contra las amenazas comunes a nuestra seguridad. La gran fuerza de nuestra relación queda patente en el alcance de nuestros intercambios comerciales y en nuestra sólida cooperación en asuntos mundiales.

La transferencia y el intercambio de datos personales constituyen un elemento fundamental, en el que se sustentan los estrechos vínculos existentes entre la Unión Europea (UE) y los Estados Unidos (EE.UU.) tanto en el ámbito comercial como en el de las funciones coercitivas. Estos intercambios de datos exigen un elevado nivel de protección y las correspondientes salvaguardias.

En junio de 2013, las noticias sobre la existencia de extensos programas de recogida de información de inteligencia en los Estados Unidos causaron gran inquietud, en la UE y en los Estados miembros, por las consecuencias que podría tener, para los derechos fundamentales de los europeos, el tratamiento de datos personales a gran escala por parte tanto de autoridades públicas como de empresas privadas en los Estados Unidos.

Frente a ello, el 27 de noviembre de 2013 la Comisión publicó una Comunicación titulada «Restablecer la confianza en los flujos de datos entre la UE y EE.UU.[1]», con un plan de acción para recuperar la confianza en las transferencias de datos, en beneficio de la economía digital, la protección de los derechos individuales de los europeos y las relaciones transatlánticas en general. En la Comunicación se proponen las siguientes acciones clave para lograr dichos objetivos:

i) adoptar el paquete de reforma de la protección de datos propuesto por la Comisión en 2012[2];

ii) incrementar la seguridad del régimen de «puerto seguro», a partir de las trece recomendaciones expuestas en la Comunicación al respecto[3]; y

[1] Comunicación de la Comisión al Parlamento Europeo y al Consejo «Restablecer la confianza en los flujos de datos entre la UE y EE.UU.» [COM(2013) 846 final], de 27.11.2013 (en lo sucesivo, «la Comunicación de 2013» o «la Comunicación»), disponible en: http://ec.europa.eu/justice/data-protection/files/com_2013_846_en.pdf.

[2] Propuesta de Directiva del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y la libre circulación de dichos datos, COM(2012) 10 final, de 25.1.2012, y propuesta de Reglamento del Parlamento Europeo y del Consejo 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 (Reglamento general de protección de datos), COM(2012) 11 final, de 25.1.2012, disponibles en: http://ec.europa.eu/justice/data-protection/reform/index_en.htm

iii) reforzar las salvaguardias en la protección de datos cuando se trate de cooperación en el ámbito de las funciones coercitivas, concluyendo la negociación del Acuerdo marco sobre la protección de datos UE-EE.UU. Este Acuerdo se fijaba también el objetivo de lograr que los Estados Unidos se comprometieran a respetar los derechos de los ciudadanos, e incluía vías para presentar recursos judiciales, sobre todo mediante la adopción de una Ley de Recurso Judicial, que ampliara a los ciudadanos de la UE determinados derechos que la Ley de Protección de la Privacidad de los EE.UU. de 1974 concede solamente a los ciudadanos estadounidenses y los residentes permanentes.

Estos objetivos fueron reiterados en las orientaciones políticas[4] de la Comisión Juncker: «*La protección de datos es un derecho fundamental que reviste especial importancia en la era digital. Además de finalizar rápidamente la labor legislativa sobre las normas comunes de protección de los datos en el seno de la Unión Europea, también hemos de defender este derecho en nuestras relaciones exteriores. A la luz de las recientes revelaciones sobre vigilancia masiva, socios estrechos como los Estados Unidos deben convencernos de que el actual régimen de «puerto seguro» es realmente seguro si desean que se mantenga. Los Estados Unidos también deben garantizar que todos los ciudadanos de la UE tengan derecho a hacer cumplir los derechos de protección de datos en los órganos jurisdiccionales de los Estados Unidos, con independencia de que residan o no en el territorio estadounidense. Se trata de un aspecto esencial para recuperar la confianza en las relaciones transatlánticas.*».

La Comisión ha seguido trabajando para lograr estos objetivos. Aceleró las negociaciones sobre el Acuerdo marco, que fue rubricado por las Partes el 8 de septiembre de 2015. Los debates interinstitucionales al respecto se intensificaron y dieron como resultado un acuerdo político entre el Consejo y el Parlamento Europeo el 15 de diciembre de 2015. Por lo que se refiere a las transferencias de datos transatlánticas en el ámbito comercial, en enero de 2014 la Comisión inició conversaciones con EE.UU. para reforzar el régimen de puerto seguro. La anulación de la Decisión sobre puerto seguro por el Tribunal de Justicia en la sentencia *Schrems*, el 6 de octubre de 2015[5], confirmó la necesidad de un nuevo marco y amplió las directrices sobre las condiciones que este debe reunir. A raíz de la sentencia, el 6 de noviembre de 2015 la Comisión emitió directrices para las empresas, detallando instrumentos alternativos para la transmisión continuada de datos personales a los Estados Unidos[6]. El 2 de febrero de 2016, se alcanzó un acuerdo político sobre un nuevo marco para los flujos

---

[3] 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 [COM(2013) 847 final de 27.11.2013, pp. 18-19] (en lo sucesivo, «la Comunicación de puerto seguro»), disponible en: http://ec.europa.eu/justice/data-protection/files/com_2013_847_en.pdf

[4] Un nuevo comienzo para Europa: Mi Agenda en materia de empleo, crecimiento, equidad y cambio democrático. Orientaciones políticas para la próxima Comisión Europea.

[5] Sentencia de 6 de octubre de 2015 en el asunto C-362/14 Maximilian Schrems / Data Protection Commissioner, UE:C:2015:650.

[6] Véase la Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre la transferencia de datos personales de la UE a los Estados Unidos de América con arreglo a la Directiva 95/46/CE tras la sentencia del Tribunal de Justicia en el asunto C-362/14 (*Schrems)*,COM(2015) 566 final de 6.11.2015. Véase también la Declaración del Grupo de Trabajo del artículo 29 sobre las consecuencias de la sentencia *Schrems*, de 3 de febrero de 2016, disponible en: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160203_statement_consequences_schrems_judgement_en.pdf

transatlánticos de datos, el Escudo de la privacidad UE-EE.UU.[7], que sustituiría al régimen anterior.

Estos avances serán beneficiosos para las relaciones transatlánticas y restablecerán la confianza de los europeos en la economía digital, reforzando al mismo tiempo sus derechos fundamentales. Asimismo, dotarán a la UE y a sus Estados miembros de un marco jurídico de protección de datos reforzado, que conducirá a una mayor integración del mercado interior, en especial del mercado único digital, y también permitirá a la UE intensificar sus esfuerzos para promover y crear normas internacionales de protección de los datos personales y la privacidad.

Al mismo tiempo, se pusieron en marcha importantes iniciativas que han dado lugar a cambios significativos en el ordenamiento jurídico de los Estados Unidos. El 17 de enero de 2014, el presidente Obama anunció[8] reformas en la inteligencia de señales, que quedaron plasmadas en la Directiva Presidencial 28 (PPD-28)[9]. Es importante señalar que estas reformas amplían determinados aspectos de la protección de la privacidad a los ciudadanos no estadounidenses y reorientan la recogida de datos, pasando de la recogida indiscriminada a un enfoque más selectivo. La Comisión acogió favorablemente estas nuevas orientaciones al considerar que eran un paso importante en la buena dirección[10]. Este proceso de reforma repercutió favorablemente en las conversaciones con los Estados Unidos sobre el Escudo de la privacidad UE-EE.UU. Desde entonces se han introducido más cambios. Por ejemplo, en junio de 2015 los Estados Unidos adoptaron la Ley de Libertad[11], que modifica algunos de sus programas de supervisión, refuerza el control judicial y aumenta la transparencia sobre su uso. Por último, el 10 de febrero de 2016, el Congreso de los Estados Unidos aprobó la Ley de Recurso Judicial, promulgada por el presidente Obama el 24 de febrero de 2016[12].

Es en este contexto que la presente Comunicación analiza hasta qué punto se han logrado los objetivos formulados en la Comunicación de 2013. Asimismo, hace hincapié en los ámbitos en que es preciso seguir trabajando para consolidar y restablecer plenamente la confianza en los flujos transatlánticos de datos.

2. La reforma de la protección de datos en la UE

2.1 El contexto

Para aprovechar las oportunidades y hacer frente a los retos de un mundo digital cada vez más interconectado, en enero de 2012 la Comisión Europea presentó un conjunto de medidas de reforma de la protección de datos («la reforma»). Al reforzar las normas internas y conceder a los ciudadanos un mayor control sobre sus datos personales, la reforma busca aumentar la

[7] Véase http://europa.eu/rapid/press-release_IP-16-216_en.htm?locale=en
[8] https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence
[9] https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities
[10] http://europa.eu/rapid/press-release_MEMO-14-30_en.htm
[11] Ley de Libertad de 2015. L., No. 114-23, § 401, 129 Stat. 268.
[12] H.R.1428 — Ley de Recurso Judicial de 2015. Entrará en vigor 90 días después de su promulgación.

confianza en la economía digital, independientemente de que los datos personales se traten en un Estado miembro, en la UE o en terceros países como los Estados Unidos.

El conjunto de medidas de reforma consta de dos instrumentos jurídicos, un Reglamento general de protección de datos[13] (en lo sucesivo, el Reglamento), que establece un marco común de la UE para la protección de datos, y una Directiva sobre protección de datos en el ámbito de la cooperación policial y judicial (la Directiva de policía)[14]. Al proponer un Reglamento, que será directamente aplicable en los Estados miembros, la Comisión desea fijar una norma de protección de datos común a todos, eliminando con ello las diferencias en el nivel de protección entre los Estados miembros. Del mismo modo, la Directiva de policía establece por primera vez una serie de normas comunes a escala de la UE, al tiempo que tiene en cuenta las particularidades de las tradiciones judiciales y policiales en los Estados miembros.

El 15 de diciembre de 2015, el Parlamento Europeo y el Consejo llegaron a un acuerdo político sobre el paquete de reformas, cumpliendo así una de las principales acciones fijadas en la Comunicación de 2013.

2.2 ¿Qué ha cambiado?

El Reglamento actualiza, moderniza y en algunos casos refuerza los principios de la protección de datos consagrados en la Directiva[15] sobre protección de datos de 1995 para garantizar el derecho a la privacidad. Se centra en el refuerzo de los derechos individuales, la profundización del mercado interior de la UE, un cumplimiento más estricto de la normativa, la racionalización de las transferencias internacionales de datos personales, y el establecimiento de normas de protección de datos a escala mundial. Estas normas están concebidas para garantizar que los datos personales de los ciudadanos de la UE están protegidos, con independencia del lugar al que se remitan, o en el que se traten o almacenen, incluso fuera de la UE, como ocurre a menudo en el mundo digital. Una serie de características de la reforma merecen ser destacadas.

En primer lugar, su **ámbito territorial**. El Reglamento deja claro que también se aplica a las empresas establecidas en un tercer país que ofrecen bienes y servicios, o efectúan un seguimiento de la conducta de los ciudadanos, en la UE. Las empresas con sede fuera de la UE deberán aplicar las mismas normas que las empresas con sede en la UE. De esta manera se garantiza una protección global de los derechos de los ciudadanos de la UE. También crea unas condiciones equitativas, evitando desequilibrios competitivos entre empresas de la UE y empresas extranjeras que operen en la UE o que se dirijan a consumidores de la UE.

En segundo lugar, una **aplicación más estricta** de las normas de protección de datos. El Reglamento prevé un régimen de sanciones eficaz, al armonizar las competencias de las autoridades nacionales de control de la protección de datos (APD). Estas autoridades podrán

[13] COM(2012) 11 final de 25.1.2012. Véase la nota 2.
[14] COM(2012) 10 final de 25.1.2012. Véase la nota 2.
[15] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, DO L 281, de 23.11.1995, p. 31 (Directiva de protección de datos).

imponer multas de hasta 20 millones de euros o hasta el 4 % del volumen mundial de negocios anual de una empresa. Esta facultad de imponer sanciones disuasorias por incumplimiento de las normas de protección de datos, junto con el ámbito de aplicación territorial mencionado, supondrá un importante incentivo para el cumplimiento de la legislación de la UE por parte de las empresas que desarrollan su actividad en la UE. Las nuevas normas también fijan responsabilidades más claras y rigurosas para los responsables y los encargados del tratamiento de datos.

En tercer lugar, **normas armonizadas para la cooperación en ámbitos coercitivos**. La Directiva de policía aplicará los principios y normas generales sobre protección de datos al tratamiento de datos personales en ámbitos penales por parte de las autoridades policiales y judiciales de los Estados miembros. Esto incluye normas armonizadas para las transferencias internacionales de datos personales en ámbitos penales[16]. La nueva Directiva reforzará el nivel de protección de los ciudadanos, garantizando al mismo tiempo que los datos de las víctimas, los testigos y los sospechosos de delitos sean debidamente protegidos en el marco de una investigación penal o de una actuación coercitiva. La supervisión queda garantizada por autoridades nacionales de protección de datos independientes y deberá ofrecerse a los ciudadanos medios de recurso efectivos. Al mismo tiempo, unas normas más armonizadas facilitarán la cooperación de las autoridades policiales y judiciales, tanto entre Estados miembros como entre los Estados miembros y sus socios internacionales, permitiendo luchar más eficazmente contra la delincuencia y el terrorismo. Esta es una parte esencial de la Agenda Europea de Seguridad[17].

En cuarto lugar, **normas estrictas para transferencias internacionales más seguras.** Tanto el Reglamento como la Directiva de policía fijan normas transparentes, detalladas y exhaustivas en materia de transferencia de datos personales a terceros países. Estas normas abarcan todas las formas de las transferencias internacionales, ya sean comerciales o con fines coercitivos, entre particulares o autoridades públicas o entre entidades privadas y autoridades públicas. Si bien la arquitectura de las normas sobre transferencias internacionales sigue siendo esencialmente la misma que en la actual Directiva sobre protección de datos (es decir, decisiones de adecuación, cláusulas contractuales tipo y normas corporativas vinculantes, así como determinadas excepciones a la prohibición general de transferir datos personales fuera de la UE), la reforma aclara y simplifica distintos aspectos y reduce los trámites burocráticos. Asimismo se introducen algunos nuevos instrumentos para las transferencias internacionales.

El Reglamento también refuerza los **poderes de las autoridades de protección de datos de la UE**, entre otras cosas en lo que se refiere a las transferencias internacionales. En comparación con la actual Directiva sobre protección de datos, las disposiciones acerca de la independencia, las funciones y las competencias de las APD de la UE se especifican con

[16] A diferencia de la Decisión marco 2008/977/JAI del Consejo, de 27 de noviembre de 2008, relativa a la protección de datos personales tratados en el marco de la cooperación policial y judicial en materia penal, que solo regula el comercio transfronterizo de datos entre las autoridades competentes de los Estados miembros, la aplicación de estas normas con arreglo a la Directiva de policía dejará de estar supeditada a que previamente se hayan intercambiado los datos entre las autoridades policiales y judiciales penales de los Estados miembros.

[17] Véase la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones,Agenda Europea de Seguridad, COM(2015) 185 final, de 28.4.2015.

mayor detalle y se refuerzan sustancialmente. Esto incluye expresamente la facultad de suspender los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional. La Directiva de policía contiene disposiciones similares en relación con las transferencias internacionales y las competencias de las APD en relación on los organismos con funciones coercitivas.

Más concretamente, por lo que se refiere a las normas sobre las **decisiones de adecuación** de la Comisión, el Reglamento prevé un catálogo preciso y detallado de los elementos que la Comisión debe tener en cuenta al evaluar el nivel de protección de datos previsto en el ordenamiento jurídico de un tercer país. Este proceso consiste en una evaluación global que ha de efectuar la Comisión y que debe incluir las normas relativas al acceso a datos personales por parte de las autoridades públicas de un tercer país, lo cual está en consonancia con la sentencia *Schrems*. Otra característica esencial de esta evaluación es que los ciudadanos dispongan de derechos de protección de datos eficaces y cuya aplicación se garantice, y puedan obtener una reparación efectiva por vía administrativa o judicial.

Por otra parte, el Reglamento establece expresamente que la Comisión **revise periódicamente**, al menos cada cuatro años, todas sus decisiones de adecuación con el fin de mantenerse al día de todas las novedades pertinentes en un tercer país que puedan repercutir directamente, máxime si tuvieran una repercusión negativa, en el nivel de protección de su ordenamiento jurídico. Esta supervisión continua de la adecuación será un proceso más dinámico y supondrá también un diálogo con las autoridades del tercer país.

Por lo que respecta a las transferencias a terceros países en los que no existe ninguna decisión de adecuación, el Reglamento establece las condiciones para el uso de **instrumentos alternativos de transferencia** como, por ejemplo, cláusulas contractuales tipo y normas corporativas vinculantes. Añade también otros instrumentos para transferencias, tales como códigos de conducta y mecanismos de certificación aprobados. Por último, clarifica las situaciones en las que pueden utilizarse **excepciones**.

2.3 Siguientes etapas

La reforma de la protección de datos es un paso esencial para reforzar los derechos fundamentales de los ciudadanos en la era digital y facilitar la actividad empresarial al simplificar las normas para las empresas en el mercado único digital. La confianza de los consumidores en los operadores de la UE y de terceros países aumentará y, de este modo, se favorecerá la economía digital europea y mundial. Tendrá efectos positivos en nuestras relaciones comerciales con los Estados Unidos, nuestro mayor socio comercial. Aportará claridad y un entorno estable para las empresas de la UE y de otros países. Por su parte, las empresas estadounidenses se beneficiarán de la seguridad jurídica que ofrece un área económica integrada, que aplica una normativa uniforme sobre protección de datos.

La existencia de normas comunes a todos los organismos con funciones coercitivas garantizará que los datos personales estén mejor protegidos y que los ciudadanos dispongan de un derecho de recurso efectivo. Facilitar la cooperación transfronteriza entre las autoridades policiales y judiciales en los Estados miembros aumentará la eficacia en el ámbito

penal y, de esta forma, se crearán condiciones para una prevención más eficaz de la delincuencia en la UE. Al mismo tiempo, todo ello facilitará una cooperación más fluida con terceros países.

Se espera que la adopción formal del conjunto de medidas de reforma por el Parlamento Europeo y el Consejo se realice en el primer semestre de 2016. El Reglamento será aplicable dos años después de su adopción, mientras que la Directiva de policía establece un período de dos años para su incorporación a los ordenamientos jurídicos nacionales. El período transitorio de dos años debe ser utilizado por todas las partes interesadas, tanto dentro como fuera de la UE, para adaptarse a la nueva normativa. La Comisión cumplirá con su responsabilidad. Durante este período transitorio, la Comisión colaborará estrechamente con los Estados miembros, las autoridades de protección de datos y otras partes interesadas para garantizar una aplicación uniforme de las normas y la preparación del entorno para facilitar el cumplimiento.

3. LA CUMBRE UE-EE.UU. SOBRE EL ESCUDO DE LA PRIVACIDAD: UN NUEVO MARCO TRANSATLÁNTICO PARA LOS FLUJOS DE DATOS PERSONALES

3.1 El contexto

Con el fin de facilitar los flujos de datos personales entre la UE y los EE.UU. para los intercambios comerciales, garantizando al mismo tiempo la protección de estos datos, en 2000 la Comisión consideró que el marco de puerto seguro ofrecía un nivel adecuado de protección[18]. Por consiguiente, aunque no existía una ley general de protección de datos en los EE.UU., los datos personales podían transferirse libremente desde los Estados miembros de la UE hacia empresas de los Estados Unidos que hubieran suscrito a los principios de privacidad que estaban en la base de dicho marco.

En la Comunicación de 2013 sobre puerto seguro[19], la Comisión señaló una serie de deficiencias que se habían ido detectando en el funcionamiento del régimen, en particular la escasa transparencia por parte de las empresas en cuanto a su adhesión al sistema y la ausencia de supervisión efectiva, por parte de las autoridades de los EE.UU., del cumplimiento de los principios de la privacidad por parte de las empresas ratificantes. Además, las revelaciones sobre vigilancia a principios de este año suscitaron preocupación por lo que respecta a la escala y el alcance de determinados programas de inteligencia de los EE.UU. y el acceso de las autoridades públicas estadounidenses a los datos personales de los europeos transferidos con arreglo al régimen de puerto seguro. Teniendo en cuenta estos y

[18] Decisión 2000/520/CE de la Comisión, de 20 de julio de 2000. En esta Decisión, basada en el artículo 25, apartado 6, de la Directiva sobre protección de datos, la Comisión reconocía que los principios de puerto seguro y las explicaciones preparadas por el Departamento de Comercio de los Estados Unidos proporcionaban una protección adecuada a los efectos de la transferencia de datos personales desde la UE. El funcionamiento del régimen de puerto seguro se basaba en el compromiso y la autocertificación de las empresas adheridas al mismo. Con arreglo a la legislación estadounidense, estas normas son vinculantes para dichas entidades y su cumplimiento está controlado por la Comisión Federal de Comercio de los EE.UU.

[19] Véase la nota 3.

otros elementos[20], la Comisión llegó a la conclusión de que el régimen de puerto seguro debía revisarse. En este contexto, la Comisión formuló 13 recomendaciones[21]destinadas a reforzar y actualizar las garantías de protección de datos del marco. Estas recomendaciones se centraban en: i) fortalecer los principios sustantivos de privacidad e incrementar la transparencia de las políticas de privacidad de las empersas autocertificas de los EE.UU. que incorporan dichos principios; ii) mejorar y hacer más eficaz el control por parte de las autoridades estadounidenses del cumplimiento de los principios por las empresas; iii) facilitar mecanismos de resolución de conflictos para las reclamaciones de los ciudadanos; y iv) garantizar que el recurso a la excepción en ámbitos coercitivos y de seguridad nacional, contemplada en la Decisión de puerto seguro de 2000, se limita a lo estrictamente necesario y proporcionado.

Sobre la base de estas 13 recomendaciones, la Comisión entabló conversaciones con las autoridades estadounidenses en enero de 2014. La posterior anulación de la Decisión de puerto seguro por el Tribunal de Justicia, el 6 de octubre de 2015, confirmó la necesidad de crear un nuevo marco más sólido para los flujos transatlánticos de datos en materia de comercio. Si bien la sentencia del Tribunal se basa en las recomendaciones de 2013 de la Comisión, subraya la necesidad de establecer límites, salvaguardias y mecanismos de control judicial, con el fin de garantizar una protección continuada de los datos personales de los ciudadanos europeos, también cuando las autoridades públicas accedan a estos datos, o los utilicen, con fines de seguridad nacional, interés público o actuaciones coercitivas.

El 2 de febrero de 2016, tras dos años de intensas negociaciones, la UE y los EE.UU. llegaron a un acuerdo político sobre el nuevo marco UE-EE.UU., el Escudo de la privacidad. Este nuevo Acuerdo contiene nuevas salvaguardias importantes y ofrecerá un alto nivel de protección de los derechos fundamentales de los ciudadanos de la UE. El Acuerdo proporcionará la necesaria seguridad jurídica a las empresas de ambos lados del Atlántico que deseen mantener relaciones comerciales. También supondrá un nuevo impulso para la colaboración transatlántica.

Tras la conclusión de las negociaciones con los Estados Unidos, la Comisión presentará el nuevo acuerdo al «Grupo de Trabajo del artículo 29» (que comprende las APD de la UE) para que emita un dictamen sobre el nivel de protección ofrecido. Además, la decisión de adecuación se someterá al procedimiento de comitología antes de que se adopte. Se consultará también al Supervisor Europeo de Protección de Datos (SEPD).

3.2 ¿Qué ha cambiado?

El Escudo de la privacidad UE-EE.UU. es una respuesta contundente y efectiva tanto a las 13 recomendaciones de la Comisión como a la sentencia *Schrems*. Contiene varias mejoras importantes, en comparación con el anterior marco, con respecto a los compromisos que deben suscribir las empresas estadounidenses. También contiene nuevos e importantes compromisos y explicaciones detalladas de la legislación estadounidense y de las prácticas de

[20] Estos elementos incluían el aumento exponencial de los flujos de datos y su importancia para la economía transatlántica, así como el rápido crecimiento del número de empresas estadounidenses adheridas al régimen de puerto seguro. Véase la Comunicación sobre puerto seguro, p. 37.

[21] Comunicación sobre puerto seguro, pp. 18-19.

las autoridades de ese país. A diferencia del mecanismo anterior, el Escudo de la privacidad no abarca solo compromisos en el ámbito comercial, sino también, de forma significativa y por primera vez en las relaciones entre la UE y los Estados Unidos, en el ámbito del acceso a los datos personales por parte de las autoridades públicas, incluso con fines de seguridad nacional. Se trata de un elemento crucial y necesario, a la luz de la jurisprudencia del Tribunal, para restablecer la confianza en las relaciones transatlánticas tras las revelaciones sobre las medidas de vigilancia.

Los logros más importantes de este nuevo acuerdo pueden clasificarse en cuatro categorías principales:

En primer lugar, **obligaciones fuertes para las empresas y un control riguroso de su aplicación**. El nuevo acuerdo será más transparente y contendrá mecanismos eficaces de supervisión para garantizar que las empresas aplican las normas a las que están legalmente obligadas. Las empresas estadounidenses que quieran importar datos personales de Europa con arreglo al Escudo de la privacidad deberán someterse a rigurosas obligaciones sobre cómo se efectúa el tratamiento de datos de carácter personal y sobre cómo se garantizan los derechos individuales. Este enfoque supone condiciones más restrictivas y una mayor responsabilidad para las empresas acogidas al Escudo de la privacidad que transfieran datos de la UE, por ejemplo en actividades de subtratamiento, a terceras partes no incluidas en el marco, ya sea en los EE.UU. o en otros terceros países («transferencias ulteriores»). En cuanto a la supervisión, el Departamento de Comercio de los Estados Unidos se ha comprometido a efectuar un seguimiento riguroso y periódico de la manera en que las empresas cumplan sus compromisos y a descubrir y apartar a aquellas empresas que pretendan beneficiarse del régimen sin cumplir las condiciones que impone la adhesión. Los compromisos de las empresas son jurídicamente vinculantes y legalmente exigibles con arreglo a la legislación de los EE.UU. por la Comisión Federal de Comercio y las empresas que no los cumplan se enfrentarán a severas sanciones.

En segundo lugar, **salvaguardias y límites claros con respecto al acceso por parte de la administración estadounidense**. Por primera vez, el Gobierno estadounidense, a través del Departamento de Justicia y de la Oficina del Director de Inteligencia Nacional, en tanto que organismo encargado de supervisar la totalidad de servicios de inteligencia de los Estados Unidos, ha ofrecido a la UE garantías por escrito de que el acceso de las autoridades públicas a efectos de aplicación de la ley, seguridad nacional y otros fines de interés público estará sujeto a limitaciones, salvaguardias y mecanismos de supervisión. Los EE.UU. también crearán un nuevo mecanismo de recurso para los ciudadanos de la UE cuyos datos se traten en relación con la seguridad nacional, mediante un Defensor del Pueblo independiente de las autoridades nacionales de seguridad. El Defensor del Pueblo realizará un seguimiento de las quejas y consultas de los ciudadanos europeos con respecto al acceso por razones de seguridad nacional y tendrá que confirmar, a quienes hayan presentado una denuncia, que se ha cumplido la normativa o se han subsanado los posibles incumplimientos. Se trata de un cambio importante que se aplicará no solo a las transferencias bajo el Escudo de la privacidad, sino también a todas las transferencias a los Estados Unidos de datos personales con fines comerciales, independientemente de la base utilizada para transferir los datos.

En tercer lugar, **una protección eficaz del derecho a la privacidad de los ciudadanos de la UE con varias posibilidades de recurso**. Cualquier ciudadano que en Europa considere que sus datos han sido utilizados indebidamente con arreglo al nuevo acuerdo dispondrá de varias vías, accesibles y asequibles, para obtener una reparación, incluida la gratuidad de los organismos de resolución alternativa de litigios. Las empresas se comprometen a responder a las reclamaciones en un plazo determinado. Además, cualquier empresa que procese datos sobre recursos humanos de Europa tendrá que comprometerse a dar cumplimiento a las decisiones de la APD competente de la UE; otras empresas pueden contraer el mismo compromiso con carácter voluntario. Los ciudadanos también pueden recurrir a la autoridad de protección de datos de su país, que contará con un procedimiento formalizado para remitir quejas al Departamento de Comercio y a la Comisión Federal de Comercio para facilitar la investigación y resolución de la reclamación en un plazo razonable. Si el asunto no logra resolverse por estas vías, los ciudadanos podrán recurrir, en última instancia, al panel del Escudo de la privacidad, un mecanismo de resolución de litigios que puede tomar decisiones vinculantes y aplicables con respecto a las empresas de los EE.UU. acogidas al Escudo de la privacidad. Además, las APD de la UE podrán proporcionar asistencia a los ciudadanos para preparar su demanda. Tal como se ha mencionado, para las reclamaciones relativas a posibles accesos por parte de las autoridades de inteligencia nacional, se creará un nuevo Defensor del Pueblo, que ofrecerá vías de recurso adicionales.

En cuarto y último lugar, un **mecanismo de revisión conjunta anual**. De esta forma, la Comisión podrá supervisar periódicamente el funcionamiento de todos los aspectos del Escudo de la privacidad, incluidas las limitaciones y salvaguardias del acceso por motivos de seguridad nacional. La Comisión y el Departamento de Comercio de los Estados Unidos llevarán a cabo la revisión y contarán con la participación de las APD de la UE, las autoridades de seguridad nacional de los EE.UU. y el Defensor del Pueblo. De esta forma, se podrá exigir a los EE.UU. el cumplimiento de sus compromisos. Pero la Comisión no se limitará a estos aspectos. También se apoyará en todo tipo de fuentes de información disponibles, incluidos los informes de transparencia voluntaria por parte de las empresas sobre el alcance de las solicitudes de acceso[22]. La revisión anual va más allá de lo dispuesto en el nuevo Reglamento, que solo exige estas revisiones como mínimo cada cuatro años, lo que demuestra la voluntad de la UE y de los EE.UU. de asegurar rigurosamente su pleno cumplimiento.

Dicha revisión no se limita a un ejercicio formal sino que podrá tener consecuencias. En los casos en que las empresas o autoridades públicas de los Estados Unidos no respeten sus compromisos, la Comisión activará el procedimiento para suspender el Escudo de la privacidad. Como el Tribunal de Justicia ha destacado en la sentencia *Schrems*, una decisión de adecuación no debe quedar en letra muerta; bien al contrario, las empresas y autoridades estadounidenses deben alimentar y apoyar continuamente el marco, demostrando que cumplen

[22] Las grandes empresas estadounidenses de Internet ya elaboran estos informes, con el fin de reconquistar la confianza de sus clientes. La Ley de Libertad de los EE.UU. de 2015 autoriza la publicación de informes voluntarios sobre solicitudes de acceso, al menos dentro de determinados límites, para proteger los intereses de seguridad nacionales.

plenamente sus compromisos. Si no lo hicieran, las ventajas que supone la decisión de adecuación para las transferencias de datos dejarían de estar justificadas y serían retiradas.

3.3 Siguientes etapas

Los compromisos acordados por los EE.UU. en el marco del Escudo de la privacidad servirán de base para una nueva decisión de adecuación de la Comisión, en la que quedarán plasmados. Se anima a las empresas a empezar ya los preparativos a fin de estar en condiciones de participar en el nuevo marco tan pronto como sea posible tras la adopción de la Decisión de la Comisión. Por su parte, el Gobierno de los EE.UU. publicará sus observaciones en el Registro Federal de los EE.UU., lo que mostrará públicamente su compromiso.

El Escudo de la privacidad UE-EE.UU. exige la actuación de muchas partes:

- Las empresas estadounidenses participantes, que deben cumplir las obligaciones que impone el marco con pleno conocimiento de que se aplicará con rigor y que los incumplimientos serán sancionados. Para fortalecer la confianza de sus consumidores, también se anima a las empresas a elegir las APD de la UE como vía de resolución de reclamaciones sobre el Escudo de la privacidad , ya que los ciudadanos europeos muy probablemente recurrirán a esas autoridades. Del mismo modo, la medida en que las empresas estén dispuestas a utilizar la facultad prevista en la legislación de los EE.UU. de publicar informes de transparencia sobre las solicitudes de acceso que reciben, relacionadas con la seguridad nacional y con fines coercitivos, contribuirá a mantener la confianza en que dicho acceso se limitará a lo que sea necesario y proporcionado[23].

- Las distintas autoridades estadounidenses encargadas de supervisar y garantizar el cumplimiento del marco, respetando las limitaciones y salvaguardias en lo que respecta al acceso a los datos con fines coercitivos y de seguridad nacional, y las responsables de responder puntual y oportunamente a las reclamaciones de los ciudadanos europeos sobre el posible uso indebido de sus datos personales.

- Las APD de la UE, que desempeñan un importante papel a la hora de garantizar que los ciudadanos puedan ejercer eficazmente sus derechos en el contexto del Escudo de la privacidad, entre otras cosas canalizando sus reclamaciones a las autoridades estadounidenses pertinentes y cooperando con ellas, poniendo en marcha el mecanismo del Defensor del Pueblo, ayudando a los denunciantes a trasladar su reclamación al panel del Escudo de la privacidad, así como supervisando las transferencias de datos ligadas a recursos humanos. y

- La Comisión, responsable de las constattaciones de adecuación y de su periódica revisión. Estas revisiones periódicas son un cambio importante respecto a la estática

[23] Dicha publicación se hará de acuerdo con lo dispuesto en la Ley de Libertad de los EE.UU. de 2015. Véase la nota 22.

situación anterior, con lo que el análisis del carácter adecuado que establece el Escudo de la privacidad se convierte en una supervisión estrecha y viva.

La revisión conjunta anual y el consiguiente informe de la Comisión — así como la posibilidad de suspender el Acuerdo en caso de incumplimiento — desempeñan un papel central a la hora de garantizar que el Escudo de la privacidad mantenga su validez a lo largo del tiempo. Nuestra mutua ambición transatlántica debe lograr establecer una sólida cultura de respeto a la privacidad y de protección de los derechos individuales, que recupere la confianza y la conserve.

4. EL ACUERDO MARCO: FORTALECIMIENTO DE LAS SALVAGUARDIAS DE PROTECCIÓN DE DATOS EN LOS ÁMBITOS COERCITIVOS

4.1 El contexto

Una dimensión importante de nuestra relación transatlántica es la capacidad de la UE, los Estados miembros y los Estados Unidos para responder eficazmente, de forma cooperativa y coordinada, a amenazas y retos para la seguridad que afectan a ambas partes. Esta respuesta colectiva depende significativamente de que podamos intercambiar datos personales en el marco de la cooperación policial y judicial en materia penal. Para alcanzar este objetivo, a lo largo de los años se han ido suscribiendo varios acuerdos bilaterales, entre los Estados miembros y los EE.UU., así como entre la UE y los Estados Unidos[24]. Al mismo tiempo, es igualmente importante que estos acuerdos en ámbitos coercitivos contengan salvaguardias eficaces en materia de protección de datos. Fue ese doble objetivo — trabajar con éxito con nuestros socios de los Estados Unidos para luchar contra la gran delincuencia y el terrorismo y, a la vez, mejorar el nivel de protección de los ciudadanos europeos en consonancia con los derechos fundamentales y las normas europeas sobre protección de datos cuando se efectúan transferencias con estos fines — lo que lanzó las negociaciones, iniciadas en marzo de 2011, sobre un acuerdo internacional en materia de protección de datos en ámbitos coercitivos, el Acuerdo marco sobre la protección de datos UE-EE.UU[25].

Las negociaciones finalizaron en el verano de 2015. El Acuerdo marco fue rubricado por las dos Partes el 8 de septiembre de 2015 en Luxemburgo[26] y se encuentra a la espera de su ratificación a ambos lados del Atlántico. No obstante, la firma del Acuerdo marco estaba supeditada a la aprobación de la Ley de Recurso Judicial por el Congreso de los Estados Unidos, que por primera vez establece la igualdad de trato de los ciudadanos de la UE con los ciudadanos estadounidenses, en virtud de la Ley de Protección de la Privacidad de los Estados

[24] En particular, el Acuerdo entre la UE y los Estados Unidos sobre el registro de nombres de los pasajeros y el Acuerdo entre la UE y los Estados Unidos sobre el programa de seguimiento de la financiación del terrorismo.

[25] Un acuerdo entre la UE y los EE.UU. sobre la protección de datos personales cuando se transfieren y tratan con el fin de prevenir, investigar, detectar o perseguir delitos, incluido el terrorismo, en el marco de la cooperación policial y judicial en materia penal.

[26] http://europa.eu/rapid/press-release_STATEMENT-15-5610_en.htm

Unidos de 1974.[27] El proyecto de ley fue aprobado por el Congreso el 10 de febrero de 2016 y se promulgó el 24 de febrero de 2016.

4.2 ¿Qué ha cambiado?

El Acuerdo marco consagrará, por primera vez, un conjunto global y armonizado de salvaguardias para la protección de datos, que se aplicará a todos los intercambios transatlánticos entre las autoridades competentes de la aplicación de Derecho penal. Se trata, en efecto, de un acuerdo sobre derechos fundamentales, que fija un elevado nivel de protección, que se utilizará para evaluar todos los intercambios de datos incluidos en los acuerdos actuales así como en los futuros.

En primer lugar, **las protecciones y las salvaguardias ofrecidas por el Acuerdo marco se aplicarán horizontalmente a todos los intercambios de datos que se realicen en el marco de la cooperación transatlántica en materia penal.** Esto incluye transferencias sobre la base de leyes nacionales, acuerdos entre la UE y EE.UU., acuerdos entre Estados miembros y EE.UU. (por ejemplo, los acuerdos de asistencia judicial mutua), así como acuerdos específicos que prevean la transferencia de datos personales por entidades privadas con miras a la aplicación de la ley. De esa forma, las disposiciones acordadas aumentarán inmediatamente el nivel de protección ofrecido a los ciudadanos de la UE cuando se transmitan datos a los EE.UU. También aumentará la seguridad jurídica en la cooperación policial y judicial transatlántica, al garantizar que los acuerdos actuales contienen todas las protecciones necesarias y por lo tanto, no son recurribles jurídicamente.

En segundo lugar, las disposiciones incluyen todas las principales normas de protección de datos de la UE en lo que respecta al **procesamiento** (por ejemplo, la calidad e integridad de los datos, su seguridad, la responsabilidad y la supervisión), **salvaguardias y limitaciones** (por ejemplo, objeto y limitaciones de su utilización, conservación de datos, transferencia ulterior de los datos, tratamiento de datos sensibles) así como a los **derechos individuales** (acceso, rectificación, recursos administrativos y judiciales).

En tercer lugar, el Acuerdo garantizará la disponibilidad de **vías de recurso judicial ante la denegación de acceso, la denegación de rectificación y la divulgación ilícita.** Se trata de una importante mejora que contribuirá de forma significativa a recuperar la confianza en los intercambios transatlánticos. Esta importante y antigua aspiración de la UE, que había quedado sin respuesta durante muchos años, ya se ha reflejado en la Ley de Recurso Judicial, presentada al Congreso de los Estados Unidos en marzo de 2015 y aprobada el 10 de febrero

[27] La Ley de Recurso Judicial otorga derechos a los ciudadanos de los «Países comprendidos», designados por el Gobierno estadounidense. Deben cumplirse los siguientes criterios: a) el país [u organización regional] tiene un acuerdo con los Estados Unidos sobre la protección de la privacidad en informaciones compartidas con el propósito de prevenir, investigar, detectar o perseguir delitos penales; b) el país [u organización regional] permite la transferencia de datos personales con fines comerciales, entre él y los Estados Unidos; y c) las políticas relativas a la transferencia de datos personales con fines comerciales y demandas conexas del país u organización regional no obstaculizan significativamente los intereses de seguridad nacional de los Estados Unidos.

de 2016. Dicha Ley ampliará a los ciudadanos de la UE[28] tres principales vías de recurso judicial contenidas en la Ley de Protección de la Privacidad de los Estados Unidos de 1974, actualmente reservadas únicamente a los ciudadanos estadounidenses y residentes permanentes. Así, por primera vez, los ciudadanos europeos podrán ampararse en derechos de aplicación general para cualquier transferencia transatlántica de datos en el ámbito del derecho penal. De esa forma se elimina una diferencia de trato entre los ciudadanos de la UE y de los Estados Unidos.

En cuarto lugar, el Acuerdo marco generaliza y amplía a todos los ámbitos coercitivos el principio de **supervisión independiente**, requisito fundamental de la protección de datos que no está presente en muchos de los acuerdos bilaterales existentes. Supone poderes efectivos para investigar y resolver las reclamaciones individuales sobre el cumplimiento del Acuerdo.

En quinto lugar, la aplicación efectiva del Acuerdo marco será objeto de **revisiones conjuntas periódicas.** En esas evaluaciones se prestará especial atención a las disposiciones relativas a los derechos de los ciudadanos (acceso, rectificación, recursos administrativos y judiciales).

El Acuerdo marco no autoriza en sí mismo las transferencias de datos, ni tampoco constituye una decisión de adecuación.

4.3 Siguientes etapas

La entrada en vigor de la Ley de Recurso Judicial[29] facilitará la firma del Acuerdo marco. Próximamente, la Comisión presentará al Consejo una propuesta de Decisión por la que se autorice la firma del Acuerdo marco. Después de la firma, el Consejo, tras obtener la aprobación del Parlamento Europeo, deberá adoptar la decisión por la que se celebra el Acuerdo. El Acuerdo marco mejorará considerablemente la situación actual, que se caracteriza por una normativa sobre protección de datos fragmentada, no armonizada y a menudo débil, conformada por un mosaico de instrumentos multilaterales, bilaterales, nacionales y sectoriales. El Acuerdo marco tiene una dimensión retrospectiva, al completar las garantías de protección de datos en los acuerdos en vigor cuando en ellos no se contemple el nivel requerido de salvaguardias. A este respecto, aportará un gran valor añadido, esencialmente al «colmar las lagunas» de los acuerdos vigentes que contienen normas de protección de datos menos estrictas que las establecidas en el Acuerdo marco. De este modo se posibilita la continuidad en la cooperación en ámbitos coercitivos, garantizando al mismo tiempo una mayor seguridad jurídica cuando se efectúen transferencias. Por lo que se refiere a los acuerdos futuros, el Acuerdo marco supondrá una «red de seguridad», ya que representa el mínimo nivel de protección exigible. Es ésta una garantía importante para el futuro y un cambio radical respecto a la situación actual, en la que las salvaguardias, la protección y los derechos tienen que negociarse en cada nuevo acuerdo. El Acuerdo marco constituye, pues, un modelo que contiene salvaguardias estandarizadas mínimas e innegociables. Este es un

[28] Según la Ley de Recurso Judicial, otros países no pertenecientes a la UE o las «organizaciones de integración económica regional» también pueden ser designados como «Países comprendidos», con la consecuencia de que un derecho de recurso judicial redundará en beneficio de sus ciudadanos.

[29] La Ley de Recurso Judicial entrará en vigor 90 días después de su adopción.

precedente muy importante no solo para las relaciones entre la UE y los Estados Unidos, sino también, más en general, para cualquier futuro acuerdo de protección o intercambio de datos a nivel internacional.

Negociado paralelamente a la reforma, el Acuerdo marco está en consonancia con el acervo de la UE en materia de protección de datos. La interacción entre la Directiva de policía y el Acuerdo marco es particularmente relevante dada la importancia de contar con un alto nivel común de protección de datos, con independencia de si los datos personales se tratan a escala nacional o se intercambian a través de las fronteras, dentro de la UE o con terceros países. A este respecto, el Acuerdo marco respalda los requisitos generales de la reforma en el contexto transatlántico.

La conclusión de las negociaciones sobre el Acuerdo marco que establece normas comunes en un ámbito complejo de la legislación y de la política es un logro significativo. El futuro Acuerdo marco permitirá restaurar y reforzar la confianza, proporcionar garantías acerca de la legalidad de las transferencias de datos y facilitar la cooperación entre la UE y los Estados Unidos en este ámbito.

De cara al futuro, es necesario abordar conjuntamente lso retos comunes en el ámbito de la cooperación policial y judicial. Una importante cuestión pendiente es el acceso directo por parte de las autoridades policiales a los datos personales en poder de las empresas privadas en el extranjero. Dicho acceso debe obtenerse, en principio, en el marco de los canales oficiales de cooperación, tales como los acuerdos de asistencia judicial mutua u otros acuerdos sectoriales. Las empresas privadas actualmente se encuentran ante una inseguridad jurídica, que podría afectar su capacidad para operar en diferentes países, ya que se les pide que faciliten el acceso a las pruebas electrónicas en virtud de las leyes de un país, para datos personales sujetos a la legislación de otro país. En paralelo a la próxima revisión del Acuerdo de asistencia judicial UE-EE.UU.[30], la UE sería muy partidaria de proseguir las discusiones con los EE.UU. al respecto, abordando entre otras cosas el desarrollo de normas comunes y más eficaces para reunir pruebas electrónicas.

5. Conclusión

La provechosa conclusión de las acciones clave esbozadas en la Comunicación de 2013 demuestra la capacidad de la UE para solucionar los problemas de forma pragmática y específica, sin por ello sacrificar su firme compromiso con los valores, tradiciones y derechos fundamentales. Asimismo, demuestra que la UE y los EE.UU. puedan resolver sus diferencias y tomar decisiones difíciles para preservar una relación estratégica que ha resistido el paso del tiempo. Al mismo tiempo, al empezar un nuevo capítulo de nuestras relaciones bilaterales, debemos mantener la vigilancia, puesto que tenemos que seguir haciendo frente a amenazas y desafíos comunes en un mundo lleno de incertidumbre.

[30] Decisión 2009/820/PESC del Consejo, de 23 de octubre de 2009 , sobre la celebración, en nombre de la Unión Europea, del Acuerdo de Extradición entre la Unión Europea y los Estados Unidos de América y del Acuerdo de Asistencia Judicial en materia penal entre la Unión Europea y los Estados Unidos de América DO L 291, 7.11.2009, p. 40-41.

Una vez que el Escudo de la privacidad y el Acuerdo marco sean efectivos, incumbe a ambas partes garantizar que estos dos importantes sistemas de transmisión de datos funcionen con eficacia y de un modo duradero. Su éxito depende en gran medida de la aplicación efectiva y el respeto de los derechos reconocidos a los ciudadanos. También depende de la evaluación continua de su funcionamiento. Para ello es necesario un cambio de perspectiva, sustituyendo el enfoque estático por otro más dinámico.

En este contexto, un elemento importante es la reforma en curso de los servicios de inteligencia de los Estados Unidos. La Comisión seguirá de cerca los próximos informes preparados por la Junta de supervisión de la privacidad y las libertades civiles y la revisión de la sección 702 del programa FISA relativo a la vigilancia extranjera prevista para 2017. También serán objeto de un estrecho seguimiento otras reformas relacionadas con la transparencia, la supervisión y la ampliación de salvaguardias a los ciudadanos no estadounidenses.

De forma más general, dada la importancia de los flujos transfronterizos de datos para el comercio transatlántico, la UE seguirá de cerca los avances legislativos por parte de los EE.UU. en materia de privacidad. Ahora que Europa se ha dotado de un único conjunto de normas coherentes y sólidas, esperamos que los Estados Unidos también proseguirán los esfuerzos para establecer un sistema integral de protección de datos y de la privacidad. Este enfoque integral podría permitir a largo plazo la convergencia entre los dos sistemas. A este respecto, la Comisión celebrará una cumbre anual sobre privacidad con ONG y otras partes interesadas a ambos lados del Atlántico.

La colaboración entre la UE y los Estados Unidos puede constituir una fuerza impulsora para desarrollar y promover normas jurídicas internacionales para la protección de la privacidad y de los datos personales. A este respecto cabe mencionar también la importancia de iniciativas emprendidas en Naciones Unidas, incluido el trabajo del Relator Especial sobre el derecho a la privacidad. En los próximos años, teniendo en cuenta la creciente importancia de estas cuestiones en la escena mundial, la UE y los Estados Unidos deben aprovechar esta oportunidad para promover sus valores comunes de libertades y derechos individuales en el mundo digital globalizado.