

Bruselas, 12 de enero de 2017
(OR. en)

5191/17

DATAPROTECT 3
JAI 18
RELEX 19
DIGIT 3
FREMP 2

NOTA DE TRANSMISIÓN

De:	secretario general de la Comisión Europea, firmado por D. Jordi AYET PUIGARNAU, director
Fecha de recepción:	12 de enero de 2017
A:	D. Jeppe TRANHOLM-MIKKELSEN, secretario general del Consejo de la Unión Europea
N.º doc. Ción.:	COM(2017) 7 final
Asunto:	COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL CONSEJO - Intercambio y protección de los datos personales en un mundo globalizado

Adjunto se remite a las Delegaciones el documento – COM(2017) 7 final.

Adj.: COM(2017) 7 final

Bruselas, 10.1.2017
COM(2017) 7 final

**COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO Y AL
CONSEJO**

Intercambio y protección de los datos personales en un mundo globalizado

1. INTRODUCCIÓN

La protección de los datos personales, consagrada en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea, forma parte de los fundamentos constitucionales comunes de Europa y lleva más de veinte años ocupando un lugar destacado en el Derecho de la Unión, desde la introducción de la Directiva sobre protección de datos en 1995¹ (en lo sucesivo, «la Directiva de 1995») hasta la adopción del Reglamento general de protección de datos² (en lo sucesivo, «RGPD») y de la Directiva de policía³ en 2016.

Tal como puso de relieve el presidente Juncker en su discurso sobre el estado de la Unión de 14 de septiembre de 2016, «[s]er europeo conlleva el derecho a que nuestros datos personales estén protegidos por estrictas leyes europeas. [...] En Europa, valoramos la intimidad: es una cuestión de dignidad humana».

Sin embargo, la exigencia de protección de los datos personales no se limita a Europa. Los consumidores de todo el mundo se muestran cada vez más celosos de su privacidad. Por su parte, las empresas reconocen que la aplicación de estrictas medidas de protección de la privacidad les otorga una ventaja competitiva al aumentar la confianza en sus servicios, y muchas de ellas, sobre todo las que operan a escala mundial, están adaptando sus políticas de privacidad al RGPD porque desean desarrollar sus actividades en la UE y porque la consideran un referente.

Asimismo, varios países y organizaciones regionales no pertenecientes a la UE, tanto de nuestra vecindad inmediata como de Asia, América Latina y África, están aprobando nuevas leyes o actualizando la legislación vigente en materia de protección de datos con objeto de aprovechar las oportunidades que brinda la economía digital mundial y satisfacer la creciente demanda de una mayor seguridad de los datos y una mayor protección de la privacidad. Si bien existen diferencias entre los distintos países en cuanto al planteamiento adoptado y al nivel de desarrollo legislativo, se observan indicios de convergencia al alza hacia importantes principios de protección de datos, sobre todo en determinadas regiones del mundo⁴. Una mayor compatibilidad entre los diversos sistemas de protección de datos facilitaría los flujos

¹ 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.

² Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), DO L 119 de 4.5.2016, pp. 1-88. Entró en vigor el 24 de mayo de 2016 y se aplicará a partir del 25 de mayo de 2018.

³ Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 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 a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, DO L 119 de 4.5.2016, pp. 89-131. Entró en vigor el 5 de mayo de 2016 y los Estados miembros de la UE han de incorporarla a su ordenamiento jurídico interno antes del 6 de mayo de 2018.

⁴ Véase UNCTAD: *Data protection regulations and international data flows: Implications for trade and development* (Normativa de protección de datos y flujos internacionales de datos: implicaciones para el comercio y el desarrollo), 2016: http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf.

internacionales de datos personales, ya sea con fines comerciales, ya sea con fines de cooperación entre las autoridades públicas (por ejemplo, en materia de aplicación de la ley). La UE debería aprovechar esta oportunidad para promover sus valores relativos a la protección de datos y facilitar la circulación de los datos mediante el fomento de la convergencia de los ordenamientos jurídicos. Por consiguiente, como ya se adelantó en el programa de trabajo de la Comisión⁵, la presente Comunicación establece el marco estratégico de la Comisión con respecto a las «decisiones de adecuación», así como otros mecanismos de transferencia de datos e instrumentos internacionales de protección de datos.

2. EL PAQUETE DE REFORMA DE LA PROTECCIÓN DE DATOS EN LA UE: UN MARCO LEGISLATIVO MODERNO QUE FAVORECE LOS FLUJOS INTERNACIONALES DE DATOS CON UN ALTO NIVEL DE PROTECCIÓN

La reforma de la legislación de la UE sobre protección de datos aprobada en abril de 2016 introduce un sistema que garantiza un elevado nivel de protección sin cerrarse a las oportunidades que ofrece la sociedad mundial de la información. Al otorgar a las personas físicas un mayor control sobre sus datos personales, la reforma refuerza la confianza de los consumidores en la economía digital. Al mismo tiempo, al armonizar y simplificar el marco jurídico permite a las empresas, tanto de la UE como de terceros países, desarrollar sus actividades económicas en la Unión en condiciones más fáciles y menos onerosas, en particular mediante intercambios internacionales de datos. En la actualidad, la UE combina la apertura a los flujos internacionales de datos con el máximo grado de protección de las personas físicas y podría convertirse en el centro neurálgico de los servicios de datos, que requieren confianza y la libre circulación de información.

2.1. Un marco de protección de datos de la UE integral, unificado y simplificado

La reforma de la UE establece un marco integral que rige el tratamiento de datos personales tanto en el sector privado como en el público y tanto en el ámbito comercial como en el de la aplicación de la ley (a través del RGPD y de la Directiva de policía, respectivamente).

En virtud del RGPD, a partir de mayo de 2018 se aplicará una normativa única paneuropea en lugar de las veintiocho legislaciones nacionales vigentes en la actualidad. Gracias al recién creado mecanismo de «ventanilla única», corresponderá a una sola autoridad de protección de datos controlar las operaciones transfronterizas de tratamiento de datos que las empresas lleven a cabo en la UE. Asimismo, se garantizará una interpretación coherente de las nuevas normas. En particular, en aquellos asuntos transfronterizos en los que intervengan varias autoridades nacionales de protección de datos, se adoptará una única decisión con el fin de asegurar que se den soluciones comunes a los problemas comunes. Por otro lado, el RGPD genera una situación de igualdad de condiciones entre las empresas de la UE y de terceros países, en el sentido de que las empresas domiciliadas fuera de la UE tendrán que aplicar las mismas normas que las empresas europeas si suministran bienes y servicios o vigilan la

⁵ Programa de trabajo de la Comisión para 2017: Realizar una Europa que proteja, capacite y vele por la seguridad, COM(2016) 710 final de 25.10.2016, p. 12 y anexo 1.

conducta de los ciudadanos en la UE. El aumento de la confianza de los consumidores beneficiará tanto a los operadores comerciales de la UE como a los de terceros países.

La Directiva de policía establece normas comunes relativas al tratamiento de los datos personales de las personas físicas implicadas en procesos penales, ya sea en calidad de sospechosos, víctimas o testigos, teniendo en cuenta el carácter específico del ámbito policial y de la justicia penal. La armonización de las normas de protección de datos en el ámbito de la aplicación de la ley, incluidas las relativas a las transferencias internacionales, facilitará la cooperación transfronteriza entre las autoridades policiales y judiciales, tanto dentro de la UE como con los socios internacionales y, de este modo, propiciará una mayor eficacia en la lucha contra la delincuencia. Se trata de una importante contribución a la Agenda Europea de Seguridad⁶.

2.2. Un renovado y diversificado conjunto de instrumentos de transferencia internacional

Desde su origen, la legislación de la UE sobre protección de datos ha proporcionado una serie de mecanismos que permiten las transferencias internacionales de datos. El objetivo primordial de estas normas es garantizar que, cuando se transfieran datos personales de ciudadanos europeos a terceros países, se mantenga el mismo nivel de protección con respecto a los mismos. A lo largo de los años, estas normas han sentado las bases de los flujos internacionales de datos en muchas jurisdicciones. Si bien la arquitectura sigue siendo, en esencia, la misma que dispuso la Directiva de 1995, la reforma de las normas relativas a las transferencias internacionales aclara y simplifica su utilización e introduce nuevos instrumentos de transferencia.

Con arreglo al Derecho de la Unión, una forma de transferir datos personales a terceros países es la que se basa en una «decisión de adecuación» de la Comisión que constate que el tercer país interesado ofrece un nivel de protección de datos «sustancialmente equivalente»⁷ al garantizado en la UE. Dicha decisión tiene por efecto permitir la libre circulación de datos personales hacia ese tercer país sin que el exportador de los datos tenga que aportar garantías adicionales ni obtener ningún tipo de autorización. La nueva normativa facilita un catálogo preciso y detallado de los elementos que la Comisión debe tener en cuenta al evaluar la adecuación del nivel de protección previsto en el ordenamiento jurídico de un tercer país o de una organización internacional⁸. Ahora la Comisión también puede adoptar decisiones de

⁶ 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.

⁷ Sentencia del Tribunal de Justicia de la Unión Europea, de 6 de octubre de 2015, en el asunto C-362/14, Maximilian Schrems / Data Protection Commissioner, (en lo sucesivo, «sentencia Schrems»), apartados 73, 74 y 96. Véanse también el considerando 104 del RGPD y el considerando 67 de la Directiva de policía, que hacen alusión a esta norma de equivalencia sustancial.

⁸ Véase el artículo 45 del RGPD. De conformidad con el artículo 45, apartado 2, la Comisión tendrá en cuenta en su evaluación, entre otros, el Estado de Derecho, el respeto de los derechos humanos y las libertades fundamentales, así como la legislación pertinente, incluida la relativa a la protección de datos, la seguridad pública, la defensa, la seguridad nacional y la legislación penal, y el acceso de las autoridades públicas a los datos personales. Estos deben estar respaldados por el reconocimiento de derechos efectivos y exigibles, entre ellos el derecho a una tutela administrativa y judicial efectiva, a los interesados, así como por la existencia y el funcionamiento efectivo de una autoridad de control independiente que garantice y haga

adecuación en el ámbito de la aplicación de la ley⁹. Asimismo, partiendo de las prácticas establecidas en la Directiva de 1995, la reforma permite expresamente la adopción de decisiones de adecuación con respecto a un determinado territorio, ámbito o sector industrial de un tercer país (lo que se denomina «adecuación parcial»)¹⁰.

A falta de una decisión de adecuación, las transferencias internacionales pueden basarse en instrumentos alternativos de transferencia que ofrezcan garantías adecuadas en materia de protección de datos¹¹. La reforma formaliza y amplía las posibilidades de utilizar instrumentos existentes, como las cláusulas contractuales tipo (en lo sucesivo, «CCT»)¹² y las normas corporativas vinculantes (en lo sucesivo, «NCV»)¹³. Por ejemplo, ahora es posible incluir CCT en los contratos celebrados entre encargados del tratamiento de la UE y encargados del tratamiento de terceros países (las denominadas «cláusulas tipo de encargado a encargado»)¹⁴. En cuanto a las NCV, que hasta la fecha se limitaban a los acuerdos entre entidades pertenecientes a un mismo grupo de empresas, ahora pueden ser invocadas por uniones de empresas dedicadas a una actividad económica conjunta, sin que estas tengan que pertenecer necesariamente al mismo grupo empresarial¹⁵. Además, la reforma reduce los trámites burocráticos al suprimir las obligaciones generales de notificación previa a las autoridades de protección de datos y autorización por estas de las transferencias a terceros países basadas en CCT o NCV¹⁶. Se trata de una importante simplificación del sistema de la UE en materia de transferencias internacionales de datos, ya que la existencia de tales obligaciones, que en la actualidad varían de un Estado miembro a otro, suele percibirse como un obstáculo significativo a la circulación de datos, sobre todo para las pequeñas y medianas empresas¹⁷.

La reforma introduce también nuevos instrumentos de transferencia internacional¹⁸. En este sentido, los responsables y encargados del tratamiento podrán utilizar, en determinadas

cumplir las normas en materia de protección de datos. También se tendrá en cuenta la adhesión a convenios jurídicamente vinculantes, en particular al Convenio del Consejo de Europa n.º 108, y la participación en sistemas multilaterales o regionales relativos a la protección de datos.

⁹ Véase el artículo 36, apartado 2, de la Directiva de policía en lo concerniente a los elementos concretos que han de tenerse en cuenta al evaluar la adecuación.

¹⁰ Véanse el artículo 45, apartado 1, del RGPD y el artículo 36, apartado 1, de la Directiva de policía.

¹¹ Véase, por ejemplo, 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 a raíz de la sentencia del Tribunal de Justicia en el asunto C-362/14 (Schrems), COM(2015) 566 final de 6.11.2015.

¹² Las CCT establecen las obligaciones de protección de datos correspondientes al exportador de la UE y al importador del tercer país.

¹³ Las NCV son normas internas adoptadas por un grupo multinacional de empresas para efectuar transferencias de datos dentro del mismo grupo empresarial a entidades ubicadas en países que no garantizan un nivel de protección adecuado. Aunque la Directiva de 1995 ya preveía el recurso a las NCV, el RGPD codifica y formaliza su función como instrumento de transferencia.

¹⁴ Véanse el artículo 46, apartado 2, letras c) y d), y el considerando 168 del RGPD.

¹⁵ Véase el artículo 46, apartado 2, letra b), el artículo 47 y el considerando 110 del RGPD.

¹⁶ Véase el artículo 46, apartado 2, del RGPD.

¹⁷ El hecho de que las obligaciones de registro supongan un obstáculo comercial para muchas empresas, y en especial para las pymes, se ha puesto de relieve, por ejemplo, en el informe de la UNCTAD (página 34).

¹⁸ Véase el artículo 46, apartado 2, letras e) y f), del RGPD.

condiciones¹⁹, códigos de conducta o mecanismos de certificación aprobados (como sellos y marcas de privacidad) para proporcionar las «garantías adecuadas», lo que debería permitir el desarrollo de soluciones mejor adaptadas a las exigencias de las transferencias internacionales, que reflejen, por ejemplo, las características y necesidades específicas de un determinado ámbito o sector industrial, o de flujos de datos concretos. Asimismo, se contempla la posibilidad de aportar garantías adecuadas para las transferencias de datos entre autoridades u organismos públicos sobre la base de acuerdos internacionales o administrativos²⁰. Por último, el RGPD expone las condiciones de aplicación de las denominadas «excepciones»²¹ (por ejemplo, la prestación de consentimiento, la ejecución de un contrato o razones importantes de interés público) en las que las entidades pueden basar sus transferencias de datos en situaciones específicas, cuando no se haya adoptado una decisión de adecuación e independientemente de la utilización de alguno de los instrumentos mencionados anteriormente. En particular, contiene una nueva, aunque limitada, excepción con respecto a las transferencias que puedan tener lugar en aras de los intereses legítimos²² de una determinada empresa.

Finalmente, la reforma faculta a la Comisión para crear mecanismos de cooperación internacional que faciliten la aplicación de la normativa de protección de datos, inclusive mediante acuerdos de asistencia mutua²³. De este modo, se reconoce la posible contribución del refuerzo de la cooperación entre las autoridades de control a escala internacional con vistas a garantizar una protección más eficaz de los derechos individuales y una mayor seguridad jurídica para las empresas.

3. TRANSFERENCIAS INTERNACIONALES DE DATOS EN EL ÁMBITO COMERCIAL: FACILITAR EL COMERCIO MEDIANTE LA PROTECCIÓN DE LA PRIVACIDAD

El respeto de la privacidad constituye un requisito para garantizar la estabilidad, seguridad y competitividad de los flujos comerciales mundiales. La privacidad no es un producto con el que se pueda negociar²⁴. Internet y la digitalización de bienes y servicios han transformado la economía mundial, y la transferencia transfronteriza de datos, incluidos los de carácter personal, figura entre las actividades cotidianas de las empresas europeas de todos los tamaños y ámbitos. Puesto que los intercambios comerciales dependen cada vez más de la circulación de datos personales, la protección y seguridad de estos últimos se ha convertido en un factor fundamental de la confianza de los consumidores. Por ejemplo, dos terceras partes de los ciudadanos europeos afirman que les preocupa no tener control sobre la información que facilitan en línea, mientras que la mitad de los encuestados temen convertirse en víctimas

¹⁹ Los responsables del tratamiento de terceros países podrán adherirse a un código de conducta o mecanismo de certificación de la UE mediante la asunción de compromisos vinculantes y exigibles, por vía contractual o mediante otros instrumentos jurídicamente vinculantes, para aplicar las garantías de protección de datos contenidas en dichos instrumentos. Véase el artículo 42, apartado 2, del RGPD.

²⁰ Véase el artículo 46, apartado 2, letra a), y apartado 3, letra b), del RGPD.

²¹ Véase el artículo 49 del RGPD.

²² Véase el artículo 49, apartado 1, párrafo segundo.

²³ Véase el artículo 50 del RGPD.

²⁴ Véase, por ejemplo, la Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones, Comercio para todos: Hacia una política de comercio e inversión más responsable, COM(2015) 497 final de 14.10.2015, p. 7.

de fraude²⁵. Al mismo tiempo, las empresas europeas que operan en determinados terceros países se enfrentan cada vez más a medidas proteccionistas que no pueden justificarse por motivos legítimos de privacidad.

Por tanto, en la era digital es imprescindible que el fomento de estrictas normas de protección de datos vaya acompañado de la facilitación del comercio internacional. Si bien la protección de los datos personales constituye un aspecto innegociable²⁶ en los acuerdos comerciales, el régimen de la UE en materia de transferencias internacionales de datos descrito anteriormente proporciona un amplio y variado conjunto de instrumentos que permite la circulación de datos en diversas situaciones, al tiempo que garantiza un elevado nivel de protección.

3.1. Las decisiones de adecuación

Las decisiones de adecuación permiten la libre circulación de datos personales desde la UE sin que el exportador de datos de la Unión tenga que aportar ninguna garantía adicional ni cumplir otras condiciones. Al constatar que el ordenamiento jurídico de un determinado país ofrece un nivel de protección adecuado, la decisión reconoce que el régimen de ese país se asemeja al de los Estados miembros de la UE. Por consiguiente, las transferencias al país interesado se asimilarán a las transmisiones de datos dentro de la Unión, lo que permitirá el acceso privilegiado de dicho país al mercado único europeo y la apertura de canales comerciales para los operadores de la UE. Como ya se ha explicado anteriormente, este reconocimiento exige por fuerza un nivel de protección comparable (o «sustancialmente equivalente»)²⁷ al garantizado en la Unión, que se constatará mediante una evaluación exhaustiva del ordenamiento jurídico del tercer país interesado, incluidas las normas que regulan el acceso de las autoridades públicas a los datos personales a efectos de aplicación de la ley, seguridad nacional y otros fines de interés público.

Por otro lado, tal como confirmó el Tribunal de Justicia en su sentencia Schrems de 2015, el principio de adecuación no exige que el ordenamiento del tercer país interesado reproduzca al pie de la letra las normas de la UE²⁸, sino que el criterio radica en si, a través de la esencia de los derechos de privacidad y su aplicación, fuerza ejecutiva y supervisión efectivas, el ordenamiento en cuestión ofrece, en su conjunto, el elevado nivel de protección exigido. De las decisiones de adecuación adoptadas hasta la fecha, se desprende que es posible que la Comisión reconozca el carácter adecuado de diversos tipos de sistemas de protección de los datos personales, que representen diferentes tradiciones jurídicas. Estas decisiones se refieren a países estrechamente vinculados con la Unión Europea y sus Estados miembros (Suiza, Andorra, las Islas Feroe, Guernesey, Jersey y la Isla de Man), a importantes socios comerciales (Argentina, Canadá, Israel y los Estados Unidos) y a países pioneros en la elaboración de leyes de protección de datos en su región (Nueva Zelanda y Uruguay).

²⁵ Eurobarómetro especial 431, *Protección de datos*, junio de 2015.

²⁶ Orientaciones políticas del presidente Juncker: *Un nuevo comienzo para Europa: mi Agenda en materia de empleo, crecimiento, equidad y cambio democrático*.

²⁷ Véase la nota a pie de página 7.

²⁸ Véase el apartado 74 de la sentencia Schrems.

Las decisiones relativas a Canadá y a los Estados Unidos constatan una adecuación «parcial». La decisión sobre Canadá se aplica exclusivamente a las entidades privadas comprendidas en el ámbito de aplicación de la *Personal Information Protection and Electronic Documents Act* (Ley canadiense relativa a la protección de la información personal y a los documentos electrónicos). La recientemente adoptada Decisión sobre el Escudo de la privacidad UE-EE. UU.²⁹ constituye un caso concreto en el que, ante la falta de una legislación general estadounidense en materia de protección de datos³⁰, las empresas participantes han de asumir compromisos con vistas a aplicar las estrictas normas de protección de datos que establece dicho régimen y que, a su vez, son exigibles en virtud del Derecho estadounidense. Asimismo, el Escudo de la privacidad se basa en las declaraciones y garantías específicas prestadas por el Gobierno de los Estados Unidos con respecto al acceso con fines de seguridad nacional³¹ que fundamentan la constatación de adecuación. La Comisión supervisará de cerca el cumplimiento de estos compromisos, que se examinará en el contexto de la revisión anual del funcionamiento del marco.

En los últimos años, un creciente número de países de todo el mundo han adoptado o están elaborando nuevas leyes en materia de protección de datos y privacidad. En 2015, fueron 109 los países que promulgaron este tipo de leyes, lo que supone un considerable aumento desde los 76 identificados a mediados de 2011³². En cuanto a los países que actualmente están en proceso de elaborar tal legislación, la cifra ronda los treinta y cinco³³. Estas leyes nuevas o actualizadas tienden a fundamentarse en un conjunto básico de principios comunes —entre los que figuran el reconocimiento de la protección de datos como derecho fundamental, la adopción de legislación general en este ámbito, la existencia de derechos individuales y exigibles en materia de privacidad y la creación de una autoridad de control independiente—, lo que brinda nuevas oportunidades, sobre todo a través de las constataciones de adecuación, para facilitar en mayor medida la circulación de los datos y garantizar al mismo tiempo el mantenimiento de un elevado nivel de protección de los datos personales.

De conformidad con el Derecho de la Unión, para poder adoptar una decisión de adecuación es preciso que existan normas de protección de datos comparables a las vigentes en la UE³⁴. Esto comprende tanto las medidas de protección sustantivas aplicables a los datos personales

²⁹ Decisión de Ejecución (UE) 2016/1260 de 12 de julio de 2016.

³⁰ La Comisión alienta a los Estados Unidos a proseguir sus esfuerzos para establecer un sistema integral de protección de datos y de la privacidad que, a largo plazo, permita la convergencia entre ambos sistemas. Véase la Comunicación de la Comisión al Parlamento Europeo y al Consejo, Los flujos transatlánticos de datos: recuperar la confianza instaurando estrictas salvaguardias, COM(2016) 117 final de 29.2.2016.

³¹ A este respecto, cabe mencionar, en particular, la aplicación de la Presidential Policy Directive 28 (Directiva de Política Presidencial 28; en lo sucesivo, «PPD-28»), que impone una serie de limitaciones y salvaguardias con respecto a las actividades de inteligencia de señales, y el nombramiento de un Defensor del Pueblo específico encargado de la tramitación de las reclamaciones presentadas por ciudadanos de la UE en este ámbito.

³² G. Greenleaf: «Global data privacy laws 2015: 109 countries, with European laws now in a minority» (Las leyes de protección de datos adoptadas en 2015 por 109 países de todo el mundo dejan en minoría las leyes europeas), informe publicado en *Privacy Laws & Business International*, n.º 133, febrero de 2015, pp. 14-17.

³³ Estudio de la UNCTAD, pp. 8 y 42 (véase la nota a pie de página 4).

³⁴ En este sentido, al evaluar la adecuación, la Comisión también tiene en cuenta las obligaciones del tercer país derivadas de convenios jurídicamente vinculantes y, en particular, su adhesión al Convenio n.º 108 y a su Protocolo adicional. Véanse el artículo 45, apartado 2, letra c), y el considerando 105 del RGPD.

como los correspondientes mecanismos de supervisión y recurso disponibles en el tercer país de que se trate.

En su marco sobre las constataciones de adecuación, la Comisión considera que deben tenerse en cuenta los siguientes criterios a la hora de determinar los terceros países con los que conviene entablar un diálogo sobre adecuación³⁵:

- i) el alcance de las relaciones comerciales (efectivas o posibles) de la UE con un determinado tercer país, incluida la existencia de un acuerdo de libre comercio o de negociaciones en curso;
- ii) la magnitud de los flujos de datos personales con origen en la UE, que reflejan lazos geográficos o culturales;
- iii) si el tercer país es pionero en el ámbito de la protección de datos y la privacidad y puede servir de modelo para otros países de su región³⁶; y
- iv) la relación política global con el tercer país en cuestión, en particular por lo que respecta al fomento de valores comunes y objetivos compartidos a escala internacional.

Sobre la base de estas consideraciones, la Comisión colaborará activamente con los principales socios comerciales de Asia Oriental y Sudoriental, empezando por Japón y Corea, durante 2017³⁷, y, dependiendo de los progresos que estos logren en la modernización de sus leyes de protección de datos, con la India, aunque también con países de América Latina, sobre todo los pertenecientes al Mercosur, y de la vecindad europea que hayan manifestado interés por obtener una constatación de adecuación. Asimismo, la Comisión acoge favorablemente las manifestaciones de interés de otros terceros países que estén dispuestos a colaborar en relación con estas cuestiones. Los debates sobre posibles constataciones de adecuación se celebran en forma de diálogos bilaterales en los que se aportan todas las aclaraciones necesarias acerca de la normativa de la UE sobre protección de datos y se estudian maneras de incrementar la convergencia de las leyes y prácticas de los terceros países interesados.

En algunos casos, en lugar de adoptar un enfoque nacional, puede resultar más adecuado recurrir a otras opciones, como la adecuación parcial o sectorial (por ejemplo, en el ámbito de los servicios financieros o de las tecnologías de la información), que puedan abarcar zonas geográficas o sectores industriales que representan una parte importante de la economía de un determinado tercer país. Esta posibilidad deberá examinarse a la luz de elementos tales como el carácter y grado de desarrollo del régimen de protección de datos (ley única, leyes múltiples o sectoriales, etc.), la estructura constitucional del tercer país de que se trate o si

³⁵ En cuanto a los países con los que interesa especialmente cooperar en materia de seguridad interior y aplicación de la ley, la Comisión estudiará la posibilidad de adoptar decisiones de adecuación específicas con arreglo a la Directiva de policía; véase el apartado 4.

³⁶ Este aspecto podría resultar de especial pertinencia en el caso de los países en proceso de transición o desarrollo, ya que la protección de los datos personales constituye un elemento fundamental del Estado de Derecho y un importante factor de la competitividad económica.

³⁷ Recientemente, Japón y Corea han adoptado nuevas leyes, o modernizado las ya existentes, para establecer sistemas de protección de datos más completos.

determinados sectores de la economía se encuentran más expuestos a flujos de datos procedentes de la UE.

La adopción de una decisión de adecuación conlleva el establecimiento de un diálogo específico y una estrecha cooperación con el tercer país interesado. Estas decisiones son documentos «vivos» que han de ser supervisados de cerca por la Comisión y adaptados en caso de que se produzcan acontecimientos que afecten al nivel de protección garantizado por el tercer país en cuestión³⁸. A tal efecto, se celebrarán revisiones periódicas, al menos cada cuatro años, con el fin de abordar los problemas que surjan e intercambiar buenas prácticas entre socios cercanos³⁹. Este enfoque dinámico se aplica también a las decisiones de adecuación ya existentes, adoptadas en virtud de la Directiva de 1995, que tendrán que revisarse si dejan de cumplir la norma aplicable⁴⁰. Por consiguiente, se invita a los terceros países interesados a que informen a la Comisión de cualquier cambio pertinente que se produzca en la legislación y en la práctica con posterioridad a la adopción de la decisión de adecuación que les concierna. Resulta fundamental garantizar la continuidad de estas decisiones con arreglo a la nueva normativa introducida con la reforma⁴¹.

Las normas de protección de datos de la UE no pueden ser objeto de negociación en el marco de un acuerdo de libre comercio⁴². Si bien los diálogos sobre protección de datos y las negociaciones comerciales con terceros países han de seguir vías distintas, las decisiones de adecuación, inclusive las de carácter parcial o sectorial, son la mejor manera de fomentar la confianza mutua y garantizar la libre circulación de datos personales, favoreciendo así los intercambios comerciales que conllevan transferencias de datos personales al tercer país interesado. Por tanto, estas decisiones pueden facilitar las negociaciones comerciales o complementar los acuerdos comerciales vigentes, de modo que puedan resultar más beneficiosos. Al mismo tiempo, al promover la convergencia del nivel de protección en la UE y el tercer país de que se trate, la constatación de adecuación reduce el riesgo de que dicho país alegue motivos de protección de datos personales para imponer requisitos injustificados de localización y almacenamiento de datos. Más allá de esto, tal como se indica en la Comunicación sobre comercio para todos, la Comisión intentará utilizar los acuerdos

³⁸ De conformidad con el artículo 45, apartados 4 y 5, del RGPD, la Comisión supervisará de manera continuada los acontecimientos acaecidos en terceros países y podrá derogar, modificar o suspender una determinada decisión de adecuación si constata que el país interesado ya no garantiza un nivel de protección adecuado.

³⁹ Artículo 45, apartado 3, del RGPD.

⁴⁰ El artículo 97, apartado 2, letra a), del RGPD, dispone asimismo que la Comisión deberá presentar al Parlamento Europeo y al Consejo un informe de evaluación en 2020.

⁴¹ A fin de extraer las consecuencias de la sentencia Schrems, según la cual la Comisión había superado los límites de sus competencias al restringir en el marco de la Decisión sobre los principios de puerto seguro las facultades de las autoridades de protección de datos de suspender o prohibir los flujos de datos, el 16 de diciembre de 2016 la Comisión adoptó una Decisión «ómnibus» modificatoria por la que se suprimen las disposiciones similares de las decisiones de adecuación vigentes y se sustituyen por disposiciones que se limitan a imponer obligaciones de información entre los Estados miembros y la Comisión en el supuesto de que una autoridad de protección de datos suspenda o prohíba las transferencias a un tercer país. La Decisión ómnibus introduce asimismo la obligación de la Comisión de supervisar los acontecimientos pertinentes acaecidos en ese tercer país. Véase el DO L 355 de 17.12.2016, p. 83.

⁴² Concretamente, una constatación de adecuación es una decisión unilateral de ejecución adoptada por la Comisión en virtud de la legislación de la UE sobre protección de datos y en función de los criterios recogidos en esta.

comerciales de la UE para fijar normas que rijan el comercio electrónico y los flujos transfronterizos de datos y abordar las nuevas formas de proteccionismo digital, respetando plenamente la normativa de la UE en materia de protección de datos y sin perjuicio de dicha normativa⁴³.

La Comisión:

- dará prioridad a los debates sobre posibles decisiones de adecuación con los principales socios comerciales de Asia Oriental y Sudoriental, empezando por Japón y Corea, en 2017, pero teniendo en cuenta asimismo a otros socios estratégicos, como la India, y también con países de América Latina, sobre todo los pertenecientes al Mercosur, y de la vecindad europea;
- supervisará de cerca el funcionamiento de las decisiones de adecuación vigentes, incluida la aplicación del marco del Escudo de la privacidad UE-EE. UU., en particular a través del mecanismo de revisión conjunta anual;
- colaborará con los países interesados en la adopción de leyes estrictas de protección de datos y les ayudará a lograr este objetivo, promoviendo su convergencia con los principios de la UE sobre protección de datos.

3.2. Mecanismos alternativos de transferencia de datos

La normativa de la UE en materia de protección de datos siempre ha reconocido que no existe un planteamiento único con respecto a las transferencias internacionales de datos y esta observación es aún más cierta a raíz de la reforma. Si bien solo podrán obtener constataciones de adecuación aquellos terceros países que cumplan los criterios pertinentes, el RGPD prevé un conjunto diverso de mecanismos suficientemente flexibles para adaptarse a distintos tipos de situaciones de transferencia. Es posible crear instrumentos que tengan en cuenta las necesidades o circunstancias particulares de determinados sectores industriales, modelos de negocio u operadores. Dichos instrumentos podrían, por ejemplo, adoptar la forma de CCT que respondan a las exigencias de un ámbito concreto, como garantías específicas para el tratamiento de datos confidenciales en el ámbito sanitario, o de un tipo específico de actividades de tratamiento extendido en determinados terceros países, como los servicios externos desarrollados para empresas europeas. A tal efecto, cabría, bien adoptar nuevos conjuntos de cláusulas tipo, bien complementar las existentes con garantías adicionales, que podrían abarcar desde medidas técnicas u organizativas hasta soluciones relacionadas con el modelo de negocio⁴⁴. También se pueden satisfacer determinadas necesidades sectoriales concretas mediante la aplicación de NCV a grupos de empresas dedicadas a una actividad económica conjunta, por ejemplo en el sector de los viajes. La elaboración de CCT de encargado a encargado o de NCV para encargados del tratamiento podría favorecer las transferencias internacionales entre ellos. Por último, nuevos mecanismos de transferencia,

⁴³ Véase la Comunicación sobre comercio para todos, p. 12 (véase asimismo la nota a pie de página 24).

⁴⁴ Véanse el artículo 46, apartado 2, letras c) y d), y el considerando 109 del RGPD, que contemplan la posibilidad de introducir adaptaciones en las cláusulas tipo aprobadas siempre que no contradigan, directa o indirectamente, dichas cláusulas ni mermen los derechos o las libertades fundamentales de los interesados.

como los códigos de conducta aprobados y las certificaciones de terceros acreditados, brindan a la industria la posibilidad de introducir soluciones adaptadas a las exigencias de las transferencias internacionales, al tiempo que se benefician de las ventajas competitivas que les otorgan, por ejemplo, los sellos o marcas de privacidad. Algunos de estos instrumentos pueden desarrollarse en forma de mecanismos para transferencias concretas o dentro de otros instrumentos más amplios para determinar el cumplimiento de todas las disposiciones del RGPD, como en el caso de los códigos de conducta aprobados.

La Comisión colaborará con la industria, la sociedad civil y las autoridades de protección de datos con miras a aprovechar al máximo el potencial del conjunto de instrumentos de transferencia internacional que ofrece el RGPD. El diálogo en curso con las partes interesadas en el contexto de la aplicación de la reforma ayudará a identificar los ámbitos prioritarios de actuación en este sentido. Entre ellos podría incluirse la finalización de trabajos ya iniciados, como la redacción de CCT de encargado a encargado, en cooperación con el Grupo de Trabajo del Artículo 29 (que en 2018 será sustituido por el Comité Europeo de Protección de Datos)⁴⁵. También se pueden desarrollar nuevos componentes de la infraestructura de cumplimiento de la UE, por ejemplo mediante la definición por parte de la Comisión de los requisitos y normas técnicas aplicables a la creación y funcionamiento de los mecanismos de certificación, incluidos los aspectos relacionados con las transferencias internacionales⁴⁶. Algunas de estas medidas pueden complementarse con colaboraciones a escala internacional, en particular con organizaciones que hayan desarrollado mecanismos de transferencia similares. Por ejemplo, se podrían estudiar formas de promover la convergencia entre las NCV en virtud del Derecho de la Unión y las normas transfronterizas de privacidad elaboradas por el Foro de Cooperación Económica Asia-Pacífico (en lo sucesivo, «APEC»)⁴⁷ por lo que respecta tanto a los criterios aplicables como al proceso de aplicación en cada sistema. Esto debería contribuir a promover unas estrictas normas de protección de datos a escala mundial, así como a salvar las diferencias entre los diversos planteamientos existentes en materia de privacidad y protección de datos, ayudar a los operadores comerciales a abrirse camino entre los diferentes sistemas y concebir políticas consecuentes.

La Comisión:

- colaborará con las partes interesadas para crear mecanismos alternativos de transferencia de datos personales adaptados a las necesidades o condiciones particulares de determinados sectores industriales, modelos de negocio u operadores.

3.3. Cooperación internacional en el ámbito de la protección de datos personales

3.3.1. Promoción de las normas de protección de datos a través de instrumentos y foros multilaterales

⁴⁵ En la actualidad no existen CCT de encargados de la UE a encargados de terceros países.

⁴⁶ Artículo 43, apartados 8 y 9, del RGPD.

⁴⁷ Véase el documento de referencia común de 2014 entre el APEC y la UE con respecto a la estructura de las NCV de la UE y al sistema de las normas transfronterizas del APEC en materia de privacidad, que compara los requisitos de cumplimiento y certificación de ambos sistemas:
http://www.apec.org/~media/Files/Groups/ECSG/20140307_Referential-BCR-CBPR-reqs.pdf.

El marco jurídico de la UE en materia de protección de datos ha servido con frecuencia de ejemplo a terceros países para legislar en este ámbito. La UE seguirá participando activamente en diálogos, tanto bilaterales como multilaterales, con sus socios internacionales al objeto de fomentar la convergencia mediante la elaboración de normas de protección de datos personales estrictas y compatibles entre sí a escala mundial. Ello contribuirá a mejorar la eficacia de la protección de los derechos de las personas físicas, al tiempo que reducirá los obstáculos a la circulación transfronteriza de los datos como elemento primordial del libre comercio.

La Comisión hace especial hincapié en la adhesión de los terceros países al Convenio n.º 108 del Consejo y a su Protocolo adicional⁴⁸. El Convenio, cuya firma no está supeditada a la pertenencia al Consejo de Europa y que ya ha sido ratificado por 50 países, inclusive de África y Sudamérica⁴⁹, es el único instrumento multilateral de carácter vinculante en materia de protección de datos. En la actualidad, se encuentra en proceso de revisión y la Comisión promoverá activamente la rápida aprobación del texto modificado con vistas a la adhesión de la UE. El texto plasmará los mismos principios que se consagran en la nueva normativa de la UE en materia de protección de datos, contribuyendo así a la convergencia hacia un conjunto de normas estrictas de protección de datos.

La reunión del G-20 en 2017 brindará a la UE una nueva oportunidad de intentar lograr la convergencia en torno al principio de esencialidad de unas estrictas normas de protección de datos para el desarrollo futuro de una sociedad mundial de la información capaz de promover la innovación, el crecimiento y la prosperidad social⁵⁰.

La Comisión espera asimismo poder colaborar con nuevos agentes destacados, como el Relator Especial de las Naciones Unidas sobre el derecho a la privacidad⁵¹ y seguir profundizando en sus relaciones de trabajo con organizaciones regionales como el APEC, a fin de fomentar una cultura mundial de respeto de los derechos de privacidad y protección de los datos personales.

Dentro de su labor más amplia de sensibilización en materia de privacidad y constitución de garantías de protección de datos a escala internacional, el 15 de noviembre de 2016 la Comisión Europea aprobó un proyecto en el marco del Instrumento de Colaboración con objeto de reforzar la cooperación con sus países socios en este ámbito⁵². Dicho proyecto contempla la financiación de actividades de formación y sensibilización, entre otros. A su vez, en el contexto de la aplicación de la reforma, la UE puede beneficiarse del intercambio de

⁴⁸ Convenio del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STCE n.º 108) y Protocolo adicional de 2001 al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las autoridades de control y a los flujos transfronterizos de datos (STCE n.º 181).

⁴⁹ Mauricio, Senegal y Uruguay han ratificado el Convenio. Además, Cabo Verde, Marruecos y Túnez han sido invitados a adherirse.

⁵⁰ Véase también la Declaración ministerial de la OCDE sobre la economía digital: Innovación, crecimiento y prosperidad social («Declaración de Cancún»), de 23 de junio de 2016.

⁵¹ Véase: <http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx>.

⁵² Decisión de Ejecución de la Comisión C(2016)7198, por la que se aprueba la segunda fase del programa de acción anual de 2016 (PAA 2016) del Instrumento de Colaboración.

buenas prácticas y de las experiencias de otros ordenamientos con nuevos desafíos en materia de protección de la privacidad y soluciones jurídicas o técnicas innovadoras, inclusive en lo concerniente a instrumentos de ejecución y cumplimiento (como los mecanismos de certificación y las evaluaciones de impacto relativas a la protección de datos) o medidas de protección centradas en determinados conjuntos de datos (por ejemplo, los datos relativos a niños).

3.3.2. Cooperación en materia de aplicación de la ley

Habida cuenta del alcance mundial de las empresas multinacionales que tratan ingentes cantidades de datos personales en un gran número de países, es cada vez más necesario reforzar la cooperación con las autoridades de control y los servicios con funciones coercitivas competentes en materia de privacidad en terceros países. A menudo, los problemas de incumplimiento de las normas de protección de datos o las violaciones de la seguridad de estos afectan simultáneamente a personas de más de una jurisdicción. En estos casos, se podría mejorar la eficacia de la protección de los interesados por medio de una actuación común. Al mismo tiempo, los agentes económicos se beneficiarían de un marco jurídico más claro en el que se desarrollaran instrumentos de interpretación y prácticas de aplicación de la ley comunes a escala mundial.

Así pues, es preciso que en el mundo conectado y sin fronteras de la circulación de datos se fortalezca la cooperación entre los servicios con funciones coercitivas⁵³. La UE está dispuesta a contribuir a ello. Como ya se ha recordado anteriormente, el RGPD faculta a la Comisión para crear mecanismos de cooperación internacional que faciliten la aplicación eficaz de la legislación relativa a la protección de datos, inclusive mediante acuerdos de asistencia mutua. En este contexto, conviene estudiar la posibilidad de confeccionar un acuerdo marco de cooperación entre las autoridades de protección de datos de la UE y los servicios con funciones coercitivas de determinados terceros países, tomando también como base la experiencia adquirida por la Comisión en otros ámbitos de aplicación de la legislación, como la competencia y la protección de los consumidores.

⁵³ Entre las redes existentes figura la Red Global de Control de la Privacidad (GPEN, por sus siglas en inglés), puesta en marcha en 2010 bajo los auspicios de la OCDE. Se trata de una red informal de autoridades de control de la privacidad, entre ellas las autoridades de protección de datos de la UE, que se encarga, entre otras cosas, de la cooperación en materia de aplicación de la ley, del intercambio de buenas prácticas para abordar problemas transfronterizos y del apoyo de iniciativas conjuntas de ejecución y campañas de sensibilización. No genera nuevas obligaciones jurídicamente vinculantes entre los participantes y se centra principalmente en facilitar la cooperación en materia de aplicación de las leyes de privacidad que rigen el sector privado. Véase <https://privacyenforcement.net/>.

La Comisión:

- promoverá la rápida aprobación del texto modificado del Convenio n.º 108 del Consejo de Europa con vistas a la adhesión de la UE y fomentará también la adhesión de terceros países;
- recurrirá a foros multilaterales, como las Naciones Unidas, el G-20 o el APEC, a fin de favorecer una cultura mundial de respeto de los derechos de protección de datos;
- creará mecanismos de cooperación internacional con los principales socios internacionales al objeto de facilitar la aplicación efectiva de la legislación.

4. UNA COOPERACIÓN MÁS EFICAZ EN MATERIA DE APLICACIÓN DE LA LEY CON SÓLIDAS GARANTÍAS DE PROTECCIÓN DE DATOS

Los intercambios de datos personales constituyen una parte integrante de la prevención, la investigación y el enjuiciamiento de las infracciones penales. En un mundo interconectado en el que la delincuencia rara vez se detiene en las fronteras nacionales, la rapidez de los intercambios de datos personales resulta fundamental para garantizar la eficacia tanto de la cooperación en materia de aplicación de la ley como de la lucha contra la delincuencia. Estos intercambios deben fundamentarse en unas sólidas garantías de protección de datos, lo que también contribuye a fomentar la confianza entre los servicios con funciones coercitivas y a reforzar la seguridad jurídica cuando se recopila o intercambia información.

Las normas previstas en la Directiva de policía en relación con las transferencias internacionales rigen los intercambios de datos entre los servicios con funciones coercitivas de la UE y de terceros países, así como, en determinadas situaciones, las transferencias de dichos servicios a otras entidades. La Directiva introduce la posibilidad de adoptar decisiones de adecuación en el ámbito de la aplicación del Derecho penal. La Comisión promoverá esta posibilidad con respecto a terceros países que reúnan los requisitos pertinentes, a saber, aquellos países con los que sea preciso mantener una cooperación estrecha y rápida en el contexto de la lucha contra la delincuencia y el terrorismo, y con los que ya se estén llevando a cabo intercambios significativos de datos personales. Sobre esta base, la Comisión dará prioridad a los debates sobre decisiones de adecuación con terceros países que constituyan socios importantes a este respecto.

Por otro lado, el acuerdo marco sobre la protección de datos UE-EE. UU.⁵⁴ celebrado en diciembre de 2016 es un buen ejemplo de cómo la cooperación en materia de aplicación de la

⁵⁴ Acuerdo entre los Estados Unidos de América y la Unión Europea sobre la protección de datos personales cuando estos se transfieran y traten a efectos de la prevención, investigación, detección o enjuiciamiento de infracciones penales, incluido el terrorismo, en el marco de la cooperación policial y judicial en asuntos

ley con un importante socio internacional puede reforzarse mediante la negociación de un sólido conjunto de garantías de protección de datos. Al complementar de forma automática los instrumentos jurídicos vigentes que sirven de base a los intercambios de datos (en particular, los acuerdos bilaterales tanto a escala de la UE como de los Estados miembros), este acuerdo marco reporta beneficios directos e inmediatos a los ciudadanos y refuerza la cooperación en materia de aplicación de la ley mediante la facilitación del intercambio de información. Asimismo, al constituir un referente para futuros acuerdos de transferencia de datos con los Estados Unidos, elimina la necesidad de renegociar una y otra vez las mismas garantías. Dicho acuerdo marco es el primer acuerdo bilateral internacional que contiene un catálogo exhaustivo de los derechos y obligaciones de protección de datos con arreglo al acervo de la UE, por lo que puede servir de base para negociar acuerdos similares con terceros países, no solo en el ámbito de la cooperación judicial y policial, sino también en otros ámbitos de la aplicación de la legislación por parte de las autoridades públicas (como la política de competencia y la protección de los consumidores), abarcando tanto los intercambios intergubernamentales como las transferencias de datos entre empresas privadas y servicios con funciones coercitivas. Asimismo, podría facilitar la celebración por la Unión de acuerdos relativos al intercambio de datos entre las agencias pertinentes de la UE (a saber, Europol y Eurojust) y terceros países⁵⁵. Por consiguiente, la Comisión estudiará la posibilidad de celebrar acuerdos marco similares con sus principales socios en materia de aplicación de la ley.

La Directiva de policía contempla asimismo la posibilidad de que, en determinadas condiciones y con sujeción a rigurosas garantías, los servicios con funciones coercitivas de la UE soliciten información directamente a empresas privadas de terceros países y transmitan datos personales (normalmente un nombre o una dirección IP) en dicha solicitud⁵⁶. En cambio, el RGPD aborda expresamente los casos en los que entidades privadas establecidas en la UE transmiten datos personales a los servicios con funciones coercitivas de un tercer país a raíz de una solicitud: tales transferencias fuera de la UE solo se autorizarán en determinadas condiciones, por ejemplo si se basan en un acuerdo internacional o cuando la comunicación sea necesaria por una razón importante de interés público reconocida por el Derecho de la Unión o de los Estados miembros⁵⁷.

Esta cooperación, que está resultando fundamental para la eficacia de la investigación y enjuiciamiento de los delitos, incluido el terrorismo, ha sido puesta de relieve por el Consejo en sus conclusiones sobre la mejora de la justicia penal en el ciberespacio. El Consejo ha pedido a la Comisión que tome medidas concretas, basadas en un planteamiento común de la UE, a fin de reforzar la cooperación con los proveedores de servicios, mejorar la eficiencia de los procedimientos de asistencia judicial y proponer soluciones a los problemas de

penales: http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf (el «acuerdo marco»).

⁵⁵ La celebración de acuerdos operativos con Europol y Eurojust también ha servido de referencia en los diálogos de liberalización de visados con determinados terceros países, por ejemplo en el contexto del diálogo en curso con Turquía.

⁵⁶ Véanse el artículo 39 y el considerando 73 de la Directiva de policía.

⁵⁷ Véanse el artículo 48 y el considerando 115 del RGPD.

determinación de la jurisdicción de ejecución en el ciberespacio⁵⁸. Estas acciones abarcan tanto los intercambios entre los servicios con funciones coercitivas y los proveedores de servicios radicados en la UE como los intercambios con las administraciones públicas y las empresas no pertenecientes a la UE. La Comisión esbozará las distintas opciones para el acceso a las pruebas electrónicas en junio de 2017, teniendo en cuenta la necesidad de una cooperación rápida y segura que se deriva de las estrictas normas sobre protección de datos de la Directiva de policía y el RGPD, tanto por lo que se refiere a las situaciones internas de la UE como por lo que se refiere a las transferencias internacionales.

Por último, de conformidad con la nueva base jurídica de Europol, la Comisión evaluará las disposiciones contenidas en los citados acuerdos de cooperación operativa de Europol con terceros, celebrados en virtud de la Decisión 2009/371/JAI del Consejo, en particular las relativas a la protección de datos⁵⁹. Además, con arreglo a lo dispuesto en la Agenda Europea de Seguridad de 2015, el futuro enfoque de la Unión sobre el intercambio de datos RNP con terceros países tendrá en cuenta la necesidad de aplicar normas coherentes y salvaguardas de derechos fundamentales específicos. La Comisión seguirá explorando soluciones jurídicamente sólidas y viables para el intercambio de datos del registro de nombres de los pasajeros (RNP) con terceros países, y contemplando, en particular, la posibilidad de crear un modelo de acuerdo sobre RNP que establezca los requisitos que deben cumplir los terceros países para recibir datos RNP de la UE. No obstante, toda futura política en este ámbito dependerá, en particular, del próximo dictamen del Tribunal de Justicia de la Unión Europea referente al acuerdo previsto entre Canadá y la Unión Europea sobre el registro de nombres de los pasajeros⁶⁰.

⁵⁸ Conclusiones del Consejo de la Unión Europea sobre la mejora de la justicia penal en el ciberespacio, de 9 de junio de 2016: http://www.consilium.europa.eu/en/meetings/jha/2016/06/cyberspace--en_pdf/. En ellas se solicita a la Comisión que presente al Consejo resultados concretos sobre estas cuestiones en junio de 2017 a más tardar, tras haberle presentado su informe sobre los progresos de tales actividades en diciembre de 2016.

⁵⁹ Véase el artículo 25, apartado 4, del Reglamento (UE) 2016/794 del Parlamento Europeo y del Consejo, de 11 de mayo de 2016, relativo a la Agencia de la Unión Europea para la Cooperación Policial (Europol) y por el que se sustituyen y derogan las Decisiones 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI y 2009/968/JAI del Consejo, DO L 135 de 24.5.2016 (pp. 53-114). A más tardar el 14 de junio de 2021, la Comisión deberá presentar un informe de evaluación sobre los acuerdos de cooperación celebrados por Europol con anterioridad al 1 de mayo de 2017.

⁶⁰ Dictamen del Tribunal de Justicia sobre el proyecto de acuerdo de 2014 entre Canadá y la Unión Europea remitido al Tribunal por el Parlamento Europeo (Dictamen 1/15). Se pidió al Tribunal que evaluara la compatibilidad de dicho proyecto de acuerdo con la Carta de los Derechos Fundamentales de la Unión Europea.

UNA COOPERACIÓN MÁS EFICAZ EN MATERIA DE APLICACIÓN DE LA LEY CON SÓLIDAS GARANTÍAS DE PROTECCIÓN DE DATOS

La Comisión:

- promoverá la posibilidad de adoptar decisiones de adecuación en virtud de la Directiva de policía con respecto a los terceros países que reúnan los requisitos pertinentes;
- promoverá la negociación de acuerdos en materia de aplicación de la ley con importantes socios internacionales, de acuerdo con el modelo previsto por el acuerdo marco entre la UE y los Estados Unidos;
- dará seguimiento a las Conclusiones del Consejo sobre la mejora de la justicia penal en el ciberespacio al objeto de facilitar el intercambio transfronterizo de pruebas electrónicas con arreglo a la normativa de protección de datos.

5. CONCLUSIÓN

La protección y el intercambio de datos personales no son mutuamente excluyentes. Un sólido sistema de protección de datos facilita la circulación de estos al fomentar la confianza de los consumidores en aquellas empresas que se preocupan por el tratamiento que dan a los datos personales de sus clientes. Así pues, el cumplimiento de unas estrictas normas de protección de datos supone una ventaja en la economía digital mundial. Lo mismo ocurre con la cooperación en materia de aplicación de la ley: las garantías de privacidad constituyen una parte integrante del intercambio rápido y eficaz de información en el ámbito de la lucha contra la delincuencia, sobre la base de la confianza mutua y de la seguridad jurídica.

Tras la finalización de la reforma de su normativa de protección de datos, la UE debería colaborar de forma proactiva con terceros países a este respecto. Asimismo, debería esforzarse por lograr una convergencia al alza de los principios de protección de datos a escala internacional a través de diálogos bilaterales y multilaterales, lo que redundaría en beneficio de ciudadanos y empresas. El nuevo marco legislativo en materia de protección de datos proporciona a la UE los instrumentos necesarios y adecuados para alcanzar estos objetivos. Partiendo del enfoque estratégico expuesto en la presente Comunicación, la Comisión colaborará activamente con los principales terceros países para estudiar la posibilidad de adoptar decisiones de adecuación, empezando por Japón y Corea en 2017, con

vistas a fomentar la convergencia normativa hacia las normas de la UE y facilitar las relaciones comerciales. Al mismo tiempo, la UE hará pleno uso de los diversos mecanismos alternativos de transferencia para preservar los derechos de protección de datos y asistir a los agentes económicos cuando se transfieran datos a países cuyo ordenamiento jurídico interno no garantice un nivel adecuado de protección de datos. También convendría recurrir a estos mecanismos para facilitar en mayor medida la cooperación entre las autoridades de control y los servicios con funciones coercitivas de la UE y sus socios internacionales. La Comisión velará por la coherencia de la dimensión interior y exterior de la política de la UE en materia de protección de datos y fomentará una rigurosa protección de datos a escala internacional con el fin de mejorar la cooperación en materia de aplicación de la ley, favorecer el libre comercio y promover normas estrictas de protección de datos personales en todo el mundo.