COMISIÓN
EUROPEA

Bruselas, 24.7.2019
COM(2019) 353 final

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

Decimonoveno Informe sobre la evolución hacia una Unión de la Seguridad genuina y efectiva

I. INTRODUCCIÓN

El presente es el decimonoveno informe sobre los nuevos progresos realizados de cara a la creación de una Unión de la Seguridad genuina y efectiva, y abarca la evolución de los acontecimientos en torno a dos pilares principales: las medidas para hacer frente al terrorismo y a la delincuencia organizada y los medios en que estos se sustentan; y el refuerzo de nuestras defensas y de la resiliencia frente a esas amenazas.

Los europeos esperan, con razón, que la Unión Europea los proteja. Desde su primer día de mandato, la Comisión Juncker ha otorgado una prioridad máxima a la seguridad. En la «Nueva agenda estratégica 2019-2024» del Consejo Europeo, el objetivo de «proteger a los ciudadanos y las libertades» figura entre las cuatro prioridades principales de la Unión[1]. El Consejo Europeo ha anunciado además que aprovechará e incrementará los esfuerzos de la Unión en la lucha contra el terrorismo y la delincuencia transfronteriza, en particular mediante la mejora de la cooperación y el intercambio de información y el desarrollo de instrumentos comunes.

Gracias a una estrecha cooperación entre el Parlamento Europeo, el Consejo y la Comisión, la UE ha realizado progresos importantes en el trabajo conjunto hacia una Unión de la Seguridad genuina y efectiva, poniendo en marcha una serie de iniciativas legislativas prioritarias y ejecutando una amplia gama de medidas no legislativas para apoyar a sus Estados miembros y mejorar la seguridad para todos los ciudadanos[2]. La Unión ha actuado con resolución para restringir el perímetro de actuación de los terroristas y los delincuentes, privando a los terroristas de los medios para perpetrar atentados mediante la prohibición de la adquisición y el uso de determinadas armas de fuego y explosivos y limitando el acceso a la financiación. La UE también ha reforzado el intercambio de información entre los Estados miembros, ha colmado las lagunas de información y eliminado los ángulos muertos, combatiendo al mismo tiempo la radicalización, protegiendo a los europeos en línea, haciendo frente a las amenazas cibernéticas y a las facilitadas por el ámbito cibernético, fortaleciendo la gestión de las fronteras exteriores de la Unión y reforzando la cooperación internacional en el ámbito de la seguridad.

Al mismo tiempo, todavía hay una serie de iniciativas prioritarias en la Unión de la Seguridad pendientes de adopción por los colegisladores. Tras la constitución de la 9.ª legislatura del Parlamento Europeo de 2 de julio de 2019, el presente informe:

- establece en qué ámbitos deben actuar los colegisladores para hacer frente a las amenazas inmediatas; Es especialmente urgente **luchar contra la propaganda terrorista y la radicalización en línea**;
- determina qué iniciativas prioritarias pendientes de la Unión de la Seguridad requieren la adopción de medidas adicionales por parte de los colegisladores a fin de incrementar la **ciberseguridad**, facilitar el acceso a las **pruebas electrónicas** y completar el trabajo en materia de sistemas de información más sólidos e inteligentes para la gestión de la seguridad, las fronteras y la migración;
- información actualizada sobre el trabajo conjunto y urgente iniciado en marzo de

[1] https://www.consilium.europa.eu/media/39964/a-new-strategic-agenda-2019-2024-es.pdf

[2] Para obtener una visión general, véase la ficha «Unión de la Seguridad: una Europa que protege» (https://ec.europa.eu/commission/sites/beta-political/files/euco-sibiu-security-union_1.pdf) y el «Decimoctavo informe sobre la evolución hacia una Unión de la Seguridad genuina y efectiva» [COM(2019) 145 final, de 20.3.2019].

2019 para evaluar y reforzar la **seguridad de las redes 5G**, basándose en las evaluaciones de riesgo nacionales presentadas por los Estados miembros el 15 de julio de 2019 a más tardar;

- aborda un paquete de cuatro informes relacionados con la **lucha contra el blanqueo de capitales**, adoptados por la Comisión el 24 de julio de 2019, que analizan los actuales riesgos y vulnerabilidades en materia de blanqueo de capitales y evalúan la forma en que se está aplicando el marco normativo pertinente de la UE en los sectores público y privado;
- ofrece información actualizada sobre los progresos realizados desde marzo de 2019[3] en la ejecución de medidas legislativas de la Unión de la Seguridad, con la interoperabilidad de los sistemas de información como una de las principales prioridades para una ejecución rápida y completa por parte de los Estados miembros;
- hace balance de la labor en curso para contrarrestar la desinformación y proteger las elecciones contra las amenazas facilitadas por la cibernética, de los esfuerzos por aumentar el grado de preparación y protección contra las amenazas para la seguridad y de la cooperación con socios internacionales en materia de seguridad.

II. CUMPLIMIENTO DE LAS PRIORIDADES LEGISLATIVAS

1. Prevenir la radicalización en línea y en las comunidades

La prevención de la radicalización ocupa un lugar central en la respuesta de la UE al terrorismo, tanto en línea como en nuestras comunidades.

El atroz atentado de Christchurch (Nueva Zelanda), acaecido el 15 de marzo de 2019, sirvió de terrible recordatorio de cómo puede aprovecharse internet con fines terroristas, estén estos motivados por el yihadismo, el extremismo de ultraderecha o cualquier otra ideología extremista. La velocidad y la escala con las que el vídeo retransmitido en directo del atentado de Christchurch se propagó por las plataformas de internet pusieron de relieve la vital importancia de que las plataformas de internet dispongan de medidas adecuadas para contener la rápida difusión de tales contenidos.

En respuesta, los jefes de Estado o de Gobierno de algunos Estados miembros y de terceros países, el presidente Juncker y las plataformas en línea mostraron su apoyo, el 15 de mayo de 2019, al **«Christchurch Call to action»**[4] (Llamamiento de Christchurch), que establece medidas colectivas destinadas a eliminar los contenidos extremistas terroristas y violentos en línea. El G7[5] y el G20[6] han contraído nuevos compromisos a este respecto.

La Comisión ya ha abordado el peligro claro y actual que representa el contenido terrorista en línea mediante la **propuesta legislativa** que el presidente Juncker anunció en su discurso

---

3 Véase el Decimoctavo informe sobre la evolución hacia una Unión de la Seguridad genuina y efectiva [COM (2019) 145 final, de 20.3.2019].

4 https://www.elysee.fr/emmanuel-macron/2019/05/15/the-christchurch-call-to-action-to-eliminate-terrorist-and-violent-extremist-content-online.en. El 15 de mayo de 2019, el presidente francés, Emmanuel Macron, y la primera ministra de Nueva Zelanda, Jacinda Ardern, invitaron a París a dirigentes y plataformas en línea para poner en marcha esta iniciativa.

5 https://www.elysee.fr/en/g7/2019/04/06/g7-interior-ministers-meeting-what-are-the-outcomes

6 En el G-20 de Osaka, celebrado los días 28 y 29 de junio de 2019, los dirigentes reiteraron su compromiso de actuar para proteger a las personas del extremismo terrorista y violento conducente al terrorismo que explota las posibilidades ofrecidas por internet (https://g20.org/pdf/documents/en/FINAL_G20_Statement_on_Preventing_Terrorist_and_VECT.pdf

sobre el estado de la Unión de 2018, proponiendo un marco jurídico claro y armonizado para evitar el uso indebido de los proveedores de servicios de alojamiento de datos para la difusión de contenidos terroristas en línea[7]. Las medidas propuestas harían obligatoria para las plataformas de internet la retirada de contenidos terroristas en el plazo de una hora cuando reciban una orden de retirada de las autoridades competentes de cualquier Estado miembro. Además, cuando se esté abusando de una plataforma para propagar contenidos terroristas, tendrían la obligación de poner en práctica medidas proactivas para detectar este contenido e impedir su reaparición, aplicando normas y salvaguardias claras. Las autoridades de los Estados miembros tendrían que garantizar la existencia de un número suficiente de funcionarios encargados específicamente de hacer cumplir estas normas, que deberán contar con los recursos específicos necesarios para detectar eficazmente los contenidos terroristas y emitir órdenes de retirada.

Esto permitirá contar con un sistema rápido y efectivo a escala de la Unión y establecer salvaguardias sólidas, incluyendo mecanismos de reclamación eficaces y la posibilidad de impugnación por vía judicial.
Las medidas propuestas contribuirán a garantizar el buen funcionamiento del mercado único digital, al tiempo que se mejora la seguridad y se refuerzan la confianza en línea y las salvaguardias de la libertad de expresión y de información.

En el Consejo, los ministros de Justicia y Asuntos de Interior acordaron en diciembre de 2018 unas orientaciones generales relativas a la propuesta. El Parlamento Europeo adoptó su posición en primera lectura en abril de 2019. **La Comisión pide a ambos colegisladores que entablen lo antes posible negociaciones interinstitucionales sobre esta iniciativa prioritaria para eliminar los contenidos terroristas en línea**, con vistas a alcanzar rápidamente un acuerdo sobre un marco regulador de la UE con normas y salvaguardias claras.

Paralelamente, la Comisión prosigue la cooperación con las plataformas en línea en el marco del **Foro de la UE sobre Internet**[8]. Tal como anunció el presidente Juncker en la reunión de París de 15 de mayo de 2019, que dio lugar al Llamamiento de Christchurch, la Comisión, junto con Europol, ha iniciado los trabajos para el desarrollo de un **protocolo de crisis de la UE** que permita a los Gobiernos y a las plataformas de internet responder rápidamente y de forma coordinada a la difusión de contenidos terroristas en línea, por ejemplo, inmediatamente después de un atentado terrorista. Este trabajo forma parte de los esfuerzos realizados a nivel internacional para aplicar el Llamamiento de Christchurch. Además de nuevos debates con los Estados miembros y la industria y de un ejercicio teórico previsto para septiembre de 2019 con el fin de simular una situación de emergencia, la Comisión convocará una reunión ministerial del Foro de la UE sobre Internet para el 7 de octubre de 2019 con vistas a refrendar el protocolo de crisis de la UE.

Por otra parte, la Comisión prosigue sus esfuerzos por apoyar a los **Estados miembros y a los actores locales en la prevención contra la radicalización y la lucha contra la misma** sobre el terreno en las comunidades locales de toda Europa. Esto requiere un esfuerzo a largo plazo y sostenible en el que participen todos los actores pertinentes a nivel local, nacional y de la

[7] COM(2018) 640 final de 12.9.2018.

[8] El **Foro de la UE sobre Internet**, creado en 2015, reúne a los ministros del Interior, la industria de internet y otras partes interesadas para colaborar en una asociación voluntaria cuyo objetivo es hacer frente al uso indebido de internet por parte de grupos terroristas y proteger a los ciudadanos.

UE. El **Comité de Dirección de las acciones de la Unión en materia de prevención y lucha contra la radicalización**, creado en agosto de 2018 para asesorar a la Comisión sobre cómo reforzar la respuesta política de la UE en este ámbito, celebró su segunda reunión el 17 de junio de 2019 para estudiar nuevas medidas en ámbitos prioritarios como la radicalización en los centros penitenciarios y la lucha contra las ideologías extremistas. Puesto que los profesionales de primera línea y los de base suelen ser los mejor situados para detectar las señales tempranas de alerta de la radicalización y decidir cómo responder, la **Red para la Sensibilización frente a la Radicalización**[9], financiada por la UE, sigue prestando apoyo a quienes trabajan en primera línea conectando a unos 5 000 profesionales de la sociedad civil, los colegios y la policía, así como a coordinadores nacionales y responsables políticos.

La reciente colaboración entre los profesionales de primera línea de la Red dio lugar a una comprensión más cabal de los retos que plantea el extremismo de ultraderecha. Este año, la Red para la Sensibilización frente a la Radicalización publicará fichas informativas para ayudar a los responsables políticos y a los profesionales a reconocer las formas y manifestaciones más importantes de los extremismos islamista y de ultraderecha, tales como las principales manifestaciones de su discurso, el lenguaje, las formas, los símbolos, las tipologías y las estrategias. Por último, dado que los actores locales y las **ciudades** están a la vanguardia en la prevención y la lucha contra la radicalización, la Comisión apoya las iniciativas de las ciudades para contrarrestar la radicalización. Tras una conferencia titulada «Ciudades de la UE contra la radicalización», celebrada el 26 de febrero de 2019, se celebró, el 8 de julio de 2019, la primera reunión de un grupo piloto de unas veinte ciudades, organizada por el alcalde de Estrasburgo con el fin de intensificar el intercambio de mejores prácticas y redoblar los esfuerzos de las ciudades en este ámbito.

Paralelamente, se está trabajando en el apoyo a los países socios para hacer frente a la radicalización que pueda conducir al terrorismo, en particular en las cárceles.

A fin de hacer frente a la amenaza que representan los contenidos terroristas en línea, la Comisión pide al Parlamento Europeo y al Consejo:

- que entable negociaciones sobre la propuesta legislativa sobre la prevención de la difusión de **contenidos terroristas en línea**, con vistas a alcanzar rápidamente un acuerdo sobre un marco regulador de la UE con normas y salvaguardias claras.

2. Mejora de la ciberseguridad

La ciberseguridad sigue siendo un reto clave en materia de seguridad. La UE ha realizado avances importantes[10] a la hora de hacer frente a las ciberamenazas «clásicas» orientadas a sistemas y datos, ejecutando las medidas establecidas en la Comunicación conjunta de

[9] En 2011, la Comisión estableció la **Red para la Sensibilización frente a la Radicalización** para reunir a profesionales de primera línea y de base. En 2015, la Comisión reforzó la red mediante la creación del Centro de Excelencia de la Red para la Sensibilización frente a la Radicalización con el fin de desarrollar orientaciones más específicas, prestar servicios de apoyo y asesoramiento a las partes interesadas en los Estados miembros y aumentar la experiencia y las competencias de los distintos actores. Para más información sobre las actividades de la Red para la Sensibilización frente a la Radicalización, véase: https://ec.europa.eu/home-affairs/what-we-do/networks/radicalisation_awareness_network_en.

[10] Para más información, véase el folleto «Fortalecer la ciberseguridad en la Unión Europea: resiliencia, disuasión y defensa»: https://ec.europa.eu/digital-single-market/en/news/building-strong-cybersecurity-european-union-resilience-deterence-defence.

septiembre de 2017[11] titulada «Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE». Esto incluye el Reglamento de Ciberseguridad de la UE[12], que confiere un mandato permanente a la Agencia de la Unión Europea para la Ciberseguridad, refuerza sus funciones e instituye un marco de la UE para la certificación de la ciberseguridad. La Comisión también ha abordado los requisitos específicos del sector, por ejemplo a través de su Recomendación sobre la ciberseguridad en el sector de la energía, adoptada el 3 de abril de 2019[13]. Pero el continuo incremento de la actividad de actores malintencionados contra una amplia gama de objetivos y víctimas significa que los esfuerzos por combatir la ciberdelincuencia y reforzar la ciberseguridad siguen siendo un ámbito prioritario de actuación para la UE.

El Parlamento Europeo y el Consejo aún deben alcanzar un acuerdo sobre la iniciativa prioritaria de la **Comisión para un Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y una Red de Centros Nacionales de Coordinación**[14]. La propuesta tiene por objeto apoyar las capacidades tecnológicas e industriales de ciberseguridad y aumentar la competitividad del sector de la ciberseguridad en la Unión. Ambos colegisladores adoptaron sus mandatos de negociación en marzo de 2019. Dado que no fue posible concluir las negociaciones interinstitucionales antes de que finalizara la anterior legislatura del Parlamento Europeo, este último adoptó formalmente su posición en primera lectura. Mientras tanto, continúan los debates entre los Estados miembros en el Consejo, con especial atención a la interacción entre, por un lado, el Reglamento propuesto por el que se establecen el Centro de Competencia en Ciberseguridad y la Red y, por otro, los programas Horizonte Europa y Europa Digital. **La Comisión pide a ambos colegisladores que reanuden y concluyan con celeridad las negociaciones interinstitucionales sobre esta iniciativa prioritaria para el refuerzo de la ciberseguridad.**

Mientras tanto, la Comisión continúa **apoyando la investigación y la innovación** relacionadas con la ciberseguridad, poniendo a disposición 135 millones EUR en el actual marco financiero plurianual para proyectos en ámbitos como la ciberseguridad en infraestructuras críticas, la seguridad inteligente y la gestión de la privacidad, y herramientas desarrolladas específicamente para los ciudadanos y las pymes[15]. En julio de 2019, la Comisión publicó una nueva convocatoria de propuestas en el marco del programa del Mecanismo «Conectar Europa», poniendo 10 millones EUR de financiación de la UE a disposición de actores clave reconocidos por la Directiva relativa a la seguridad de las redes y sistemas de información (Directiva SRI)[16] como, por ejemplo, los equipos de respuesta a incidentes de seguridad informática europeos, los operadores de servicios esenciales (por ejemplo, bancos, hospitales, proveedores de servicios públicos, ferrocarriles, compañías aéreas, proveedores de nombres de dominio) y diversas autoridades públicas. Por primera vez, las autoridades europeas de certificación de la ciberseguridad también pueden solicitar la participación en este programa para poder ejecutar el Reglamento de Ciberseguridad de la

---

11 JOIN(2017) 450 final de 13.9.2017.

12 El Reglamento de Ciberseguridad de la UE [Reglamento (UE) 2019/881 de 17.4.2019] introduce por primera vez normas a escala de la UE para la certificación de la ciberseguridad de productos, procesos y servicios. Por otro lado, establece un nuevo mandato permanente para la Agencia de Ciberseguridad de la UE, además de asignarle más recursos para que pueda cumplir sus objetivos. Para más información sobre la convocatoria de propuestas, véase: https://ec.europa.eu/digital-single-market/en/news/eu10-million-eu-funding-available-projects-stepping-eus-cybersecurity-capabilities-and-cross.

13 C(2019) 2400 final de 3.4.2019 y SWD(2019) 1240 final de 3.4.2019.

14 COM(2018) 630 final de 12.9.2018.

15 https://ec.europa.eu/programmes/horizon2020/en/h2020-section/cross-cutting-activities-focus-areas

16 Directiva (UE) 2016/1148 de 6.7.2016.

UE.

El 17 de mayo de 2019, el Consejo instituyó un **régimen de sanciones** que permite a la UE imponer medidas restrictivas selectivas de disuasión y respuesta a los ciberataques que constituyan una amenaza externa para la UE y sus Estados miembros. El nuevo régimen de sanciones forma parte del **conjunto de instrumentos de ciberdiplomacia de la UE**[17], un marco para una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas[18] que permite a la UE aprovechar plenamente las medidas de la política exterior y de seguridad común con el fin de disuadir y responder a las actividades informáticas malintencionadas.

Más allá de las amenazas cibernéticas dirigidas contra sistemas y datos, la UE también está tomando medidas para hacer frente a los complejos y polifacéticos desafíos que entrañan las amenazas híbridas[19]. En sus conclusiones de 21 de junio de 2019[20], el Consejo Europeo hizo hincapié en que «la UE debe garantizar una respuesta coordinada a las amenazas híbridas y a las ciberamenazas y reforzar su cooperación con los actores internacionales pertinentes». La Comisión celebra que la lucha contra las amenazas híbridas sea también una prioridad de la Presidencia finlandesa del Consejo y que, en la reunión informal de ministros de Justicia y Asuntos de Interior que se desarrolló en los días 18 y 19 de julio de 2019 en Helsinki, haya tenido lugar un debate basado en situaciones hipotéticas sobre las políticas para hacer frente a las amenazas híbridas. También se han celebrado debates similares sobre las amenazas híbridas basados en situaciones hipotéticas entre los directores de política de defensa de la UE —el 7 y el 8 de julio de 2019— y entre los directores políticos de la UE —el 9 y el 10 de julio de 2019—. Las conclusiones de estos debates se comunicarán a los ministros de Asuntos Exteriores y de Defensa en una sesión conjunta informal el 29 y el 30 de agosto de 2019.

Con el fin de reforzar la ciberseguridad, la Comisión pide al Parlamento Europeo y al Consejo que:
• alcancen rápidamente un acuerdo sobre la propuesta legislativa relativa al **Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación**.

3. Mejora del acceso de los órganos encargados de hacer cumplir la ley a las pruebas electrónicas

17 http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/es/pdf

18 Entre estas actividades figuran los ciberataques y los intentos de ciberataques con efectos potencialmente significativos que impliquen, por ejemplo, el acceso a sistemas de información o la interceptación de datos a través de infraestructuras digitales como las redes 5G (véase también la sección III sobre el refuerzo de la seguridad de las infraestructuras digitales).

19 Véase el informe sobre la puesta en práctica del Marco común de lucha contra las amenazas híbridas de 2016 y la Comunicación conjunta sobre el incremento de la resiliencia y el refuerzo de capacidades para hacer frente a las amenazas híbridas de 2018 [SWD(2019) 200 final, de 28.5.2019]. Véase también la propuesta legislativa de septiembre de 2016 de Reglamento por el que se establece un régimen de la Unión de control de las exportaciones, la transferencia, el corretaje, la asistencia técnica y el tránsito de productos de doble uso (versión refundida) [COM(2016) 616 final, de 28.9.2016].

20 https://www.consilium.europa.eu/media/39922/20-21-euco-final-conclusions-en.pdf

La UE ha tomado medidas adicionales para privar a los terroristas y delincuentes de los medios para actuar, dificultando su acceso a los precursores de explosivos[21], la financiación de sus actividades[22] y sus desplazamientos no detectados[23].

Las negociaciones sobre las propuestas de la Comisión de abril de 2018 destinadas a mejorar el **acceso a las pruebas electrónicas** por parte de los órganos encargados de hacer cumplir la ley deben ultimarse lo antes posible, ya que, actualmente, más de la mitad de las investigaciones penales conllevan una solicitud transfronteriza de acceso a pruebas electrónicas[24]. El Consejo adoptó su posición negociadora sobre las propuestas de Reglamento[25] para mejorar el acceso transfronterizo a las pruebas electrónicas en las investigaciones judiciales y de Directiva[26] por la que se establecen normas armonizadas sobre el nombramiento de representantes legales a efectos de recabar pruebas para procesos penales. Dada la importancia crucial que reviste el acceso eficiente a las pruebas electrónicas para la investigación y el enjuiciamiento de delitos transfronterizos como el terrorismo o la ciberdelincuencia, la Comisión insta al Parlamento Europeo a impulsar esta propuesta para permitir su rápida adopción por parte de los colegisladores.

Paralelamente, la Comisión está trabajando para mejorar y garantizar las salvaguardias necesarias en el **intercambio internacional de pruebas electrónicas** en el contexto de las negociaciones en curso con vistas a un Segundo Protocolo Adicional del Convenio del Consejo de Europa sobre Ciberdelincuencia (Convenio de Budapest); asimismo, está trabajando con los Estados Unidos con arreglo a los mandatos de negociación otorgados por el Consejo en la reunión del Consejo de Justicia y Asuntos de Interior de los días 6 y 7 de junio de 2019[27]. La Comisión participó en la última ronda de negociaciones relativas al Segundo Protocolo Adicional del Convenio del Consejo de Europa sobre Ciberdelincuencia (Convenio de Budapest), celebrada del 9 al 11 de julio de 2019. Actualmente, la Comisión y las autoridades de los Estados Unidos están realizando los preparativos técnicos para el inicio formal de las negociaciones en pos de un Acuerdo UE-EE. UU. sobre el acceso transfronterizo a pruebas electrónicas.

---

21 Reglamento (UE) 2019/1148, de 20 de junio de 2019, sobre la comercialización y la utilización de precursores de explosivos.

22 Directiva (UE) 2019/1153, de 11 de julio de 2019, por la que se establecen normas destinadas a facilitar el uso de información financiera y de otro tipo para la prevención, detección, investigación o enjuiciamiento de infracciones penales.

23 Reglamento (UE) 2019/1157, de 20 de junio de 2019, sobre el refuerzo de la seguridad de los documentos de identidad de los ciudadanos de la Unión y de los documentos de residencia expedidos a ciudadanos de la Unión y a los miembros de sus familias que ejerzan su derecho a la libre circulación.

24 En alrededor del 85 % de las investigaciones judiciales se necesitan pruebas electrónicas, y en dos terceras partes de ellas es necesario solicitar pruebas de proveedores de servicios en línea establecidos en otra jurisdicción. Véase la evaluación de impacto que acompaña a la propuesta legislativa [SWD (2018) 118 final de 17.4.2018].

25 COM(2018) 225 final de 17.4.2018. El Consejo adoptó su mandato de negociación sobre la propuesta de Reglamento en el Consejo de Justicia y Asuntos de Interior celebrado el 7 de diciembre de 2018.

26 COM(2018) 226 final de 17.4.2018. El Consejo adoptó su posición negociadora sobre la propuesta de Directiva en el Consejo de Justicia y Asuntos de Interior celebrado el 8 de marzo de 2019.

27 https://www.consilium.europa.eu/es/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/

Con el fin de mejorar el acceso de los órganos encargados de hacer cumplir la ley a las pruebas electrónicas, la Comisión pide al Parlamento Europeo que:

- adopte su mandato de negociación sobre las propuestas legislativas relativas a las **pruebas electrónicas** para entablar con rapidez debates tripartitos con el Consejo. *(prioridad de la Declaración conjunta)*

4. Sistemas de información más sólidos y más inteligentes para la gestión de la seguridad, las fronteras y los flujos migratorios

Tras la adopción de normas sobre la **interoperabilidad de los sistemas de información**[28], que colmarán las lagunas de información y eliminarán los ángulos muertos al ayudar a detectar las identidades múltiples y luchar contra la usurpación de identidad, la Comisión puso en marcha rápidamente una serie de iniciativas para apoyar a los Estados miembros en el proceso de ejecución, incluso mediante la aportación de fondos en los casos necesarios, y también a través de talleres destinados a facilitar el intercambio de conocimientos especializados y mejores prácticas. La estrecha cooperación entre las agencias de la UE, la totalidad de los Estados miembros y los países asociados de Schengen será fundamental de cara a la consecución del ambicioso objetivo de lograr, de aquí a 2020, la plena interoperabilidad de los sistemas de información de la UE para la gestión de la seguridad, las fronteras y la migración.

Este objetivo requiere también una aplicación rápida y completa de la legislación recientemente acordada para establecer nuevos sistemas de información —Sistema de Entradas y Salidas de la UE[29] y Sistema Europeo de Información y Autorización de Viajes[30]—, así como para reforzar el Sistema de Información de Schengen[31] y ampliar el Sistema Europeo de Información de Antecedentes Penales[32] a nacionales de terceros países. La nueva arquitectura para unos sistemas de información más sólidos e inteligentes de gestión de la seguridad, las fronteras y la migración solo producirá resultados tangibles sobre el terreno si todos los componentes se aplican plenamente a nivel de la Unión y por cada Estado miembro, de conformidad con el calendario acordado.

Al mismo tiempo, es necesario que los colegisladores adopten nuevas medidas para completar el trabajo de implantación de sistemas de información más sólidos e inteligentes para la gestión de la seguridad, las fronteras y la migración.
En el marco de la aplicación técnica del **Sistema Europeo de Información y Autorización de Viajes**, el 7 de enero de 2019 la Comisión presentó una propuesta con las modificaciones técnicas del Reglamento correspondiente[33] que resultan necesarias para completar la implantación del sistema. La Comisión insta a los colegisladores a impulsar su labor sobre estas enmiendas técnicas a fin de llegar a un acuerdo lo antes posible, permitiendo así la aplicación rápida y oportuna del Sistema Europeo de Información y Autorización de Viajes de modo que sea operativo a principios de 2021.

---

28 Reglamento (UE) 2019/817 de 20.5.2019 y Reglamento (UE) 2019/818 de 20.5.2019.
29 Reglamento (UE) 2017/2226 de 30.11.2017.
30 Reglamento (UE) 2018/1240 de 12.9.2018 y Reglamento (UE) 2018/1241 de 12.9.2018.
31 Reglamento (UE) 2018/1860 de 28.11.2018, Reglamento (UE) 2018/1861 de 28.11.2018 y Reglamento (UE) 2018/1862 de 28.11.2018.
32 Reglamento (UE) 2019/816 de 17.4.2019.
33 COM(2019) 3 final y COM(2019) 4 final de 7.1.2019.

En mayo de 2018, la Comisión presentó una propuesta para **reforzar el actual Sistema de Información de Visados**[34], contemplando comprobaciones más exhaustivas de los antecedentes penales de los solicitantes de visado y colmando las lagunas de información mediante la mejora del intercambio de datos entre Estados miembros. El Consejo adoptó su mandato de negociación el 19 de diciembre de 2018, y el 13 de marzo de 2019 el Parlamento Europeo aprobó en sesión plenaria su informe sobre la propuesta, concluyendo así su primera lectura. La Comisión insta a los colegisladores a iniciar rápidamente sus negociaciones ahora que ya se ha constituido el nuevo Parlamento Europeo.

En mayo de 2016, la Comisión propuso extender el ámbito de aplicación de **Eurodac**[35], de modo que no solo incluya la identificación de los solicitantes de asilo, sino también la de los nacionales de terceros países que residan ilegalmente en la UE o entren en ella de forma irregular. En consonancia con las conclusiones del Consejo Europeo de diciembre de 2018[36] y la Comunicación de la Comisión de 6 de marzo de 2019 sobre el avance en la aplicación de la Agenda Europea de Migración[37], la Comisión insta a los colegisladores a proceder sin demora a la adopción de la propuesta legislativa. Es necesario adoptar esta propuesta legislativa a fin de permitir que Eurodac pase a formar parte de la futura estructura de los sistemas de información interoperables de la UE, integrando así los datos fundamentales de los nacionales de terceros países que residan ilegalmente en la UE o hayan entrado en ella de forma irregular.

Con el fin de reforzar los sistemas de información de la UE para la gestión de la seguridad, las fronteras y la migración, la Comisión insta al Parlamento Europeo y al Consejo a:

- adoptar la propuesta legislativa sobre **Eurodac** (prioridad de la Declaración conjunta);
- avanzar en la labor destinada a alcanzar rápidamente un acuerdo sobre las modificaciones técnicas propuestas necesarias para establecer el **Sistema Europeo de Información y Autorización de Viajes**.

III. REFUERZO DE LA SEGURIDAD DE LAS INFRAESTRUCTURAS DIGITALES

La resiliencia de nuestra infraestructura digital es fundamental para los Gobiernos, las empresas, la seguridad de nuestros datos personales y el funcionamiento de nuestras instituciones democráticas. Las **redes de quinta generación (5G)** que se instalarán en los próximos años constituirán la espina dorsal digital de nuestras sociedades y economías, conectando miles de millones de ciudadanos, objetos y sistemas, también en sectores críticos como la energía, el transporte, la banca y la salud, así como los sistemas de control industrial que transmiten información sensible y sirven de soporte a los sistemas de seguridad.

Con una previsión de ingresos mundiales estimados en 225 000 millones EUR en 2025, la tecnología 5G es una baza clave para que Europa compita en el mercado mundial, y **la seguridad de las redes 5G es fundamental para garantizar la autonomía estratégica de la Unión**. Para garantizar un alto nivel de ciberseguridad se requieren medidas concertadas tanto

[34] COM(2018) 302 final de 16.5.2018.
[35] COM(2016) 272 final de 4.5.2016.
[36] https://www.consilium.europa.eu/es/press/press-releases/2018/12/14/european-council-conclusions-13-14-december-2018/
[37] COM(2019) 126 final de 6.3.2019.

a nivel nacional como europeo, ya que cualquier vulnerabilidad de las redes 5G en un Estado miembro afectaría a la Unión en su conjunto.

A raíz del apoyo de los Jefes de Estado o de Gobierno expresado en el Consejo Europeo de marzo de 2019[38], la Comisión presentó, el 26 de marzo de 2019, una **Recomendación sobre la ciberseguridad de las redes 5G**[39] en la que se establecen medidas para evaluar los riesgos de ciberseguridad de las redes 5G y reforzar las medidas preventivas. Las recomendaciones se basan en una evaluación de riesgos coordinada de la UE y en medidas de gestión de riesgos, un marco eficaz para la cooperación y el intercambio de información, y una conciencia compartida de la situación en la UE en materia de redes de comunicación críticas.

Como **primera fase** del proceso iniciado por la Recomendación, a 15 de julio de 2019 todos los Estados miembros habían completado su **evaluación nacional de riesgos** y habían presentado sus conclusiones a la Comisión y a la Agencia de Ciberseguridad de la UE, o habían anunciado que lo harían en breve. Las evaluaciones nacionales de riesgos siguieron un conjunto de directrices y emplearon una plantilla común para informar sobre las conclusiones acordadas por los Estados miembros y la Comisión a fin de fomentar la coherencia y facilitar el intercambio de información sobre los resultados nacionales a escala de la UE. Entre los parámetros evaluados en todos los Estados miembros figuran:

- las amenazas y actores amenazantes principales que afectan a las redes 5G;
- el grado de sensibilidad de los componentes y funciones de la red 5G, así como de otros activos; y
- los diferentes tipos de vulnerabilidades, incluidas tanto las técnicas como las de otra índole, como, por ejemplo, las que pueden derivarse de la cadena de suministro 5G.

Además, en el trabajo de evaluación nacional de riesgos han participado una serie de actores responsables de los Estados miembros, entre ellos, en función de la asignación de responsabilidades nacional, las autoridades en materia de ciberseguridad o telecomunicaciones y los servicios de seguridad e inteligencia, lo cual ha reforzado su cooperación y coordinación. Paralelamente y teniendo en cuenta sus calendarios nacionales para la introducción de la tecnología 5G, varios Estados miembros ya han tomado medidas para reforzar los requisitos de seguridad aplicables en este ámbito, mientras que otros han manifestado su intención de estudiar nuevas medidas en un futuro próximo.

Basándose en los resultados de la evaluación nacional de riesgos, las autoridades de ciberseguridad de los Estados miembros en el Grupo de Cooperación en Redes y Sistemas de Información[40] prepararán una **revisión conjunta de los riesgos a nivel de la UE** para el 1 de octubre de 2019 a más tardar, que constituirá la segunda fase del proceso iniciado en virtud de la Recomendación. Partiendo de esta base, y ya en el contexto de la tercera fase, el Grupo de cooperación preparará, para el 31 de diciembre de 2019 a más tardar, un conjunto de medidas

[38] https://data.consilium.europa.eu/doc/document/ST-1-2019-INIT/es/pdf

[39] C(2019) 2335 final de 26.3.2019.

[40] El Grupo de Cooperación para la Seguridad de la Información en Red se ha establecido en virtud de la Directiva (EU) 2016/1148, de 6.7.2016, relativa a la seguridad de las redes y sistemas de información. Según lo previsto en la Recomendación, se ha creado una línea de trabajo específica dentro del Grupo de Cooperación para la Seguridad de la Información en Red dirigida por varios Estados miembros. El grupo se ha reunido ya en tres ocasiones —en abril, mayo y julio de 2019— para compartir información sobre los planteamientos nacionales y debatir sobre cómo facilitar la preparación de la evaluación coordinada de riesgos de la UE.

de mitigación común de la Unión para hacer frente a los riesgos detectados. La Comisión y la Agencia de Ciberseguridad de la UE seguirán apoyando la ejecución de la Recomendación.

El trabajo del Grupo de Cooperación en Redes y Sistemas de Información cuenta con el apoyo de varios foros. El Organismo de Reguladores Europeos de Comunicaciones Electrónicas está preparando un estudio sobre todas las medidas de seguridad existentes que puedan ser pertinentes para la 5G. Un nuevo grupo de expertos especializado de la Agencia de Ciberseguridad de la UE ha iniciado los trabajos para un estudio del panorama de amenazas relacionadas con la tecnología 5G. Además, tras la entrada en vigor del Reglamento sobre la Ciberseguridad el 27 de junio de 2019, la Comisión y la Agencia de Ciberseguridad de la UE tomarán todas las medidas necesarias para establecer el marco de certificación a escala de la UE. Los Estados miembros también se reunieron en junio de 2019 en el Comité de Normalización para debatir sobre la ciberseguridad y la normalización en respuesta a la Recomendación de estudiar los futuros retos a los que se enfrenta la normalización de la ciberseguridad —incluidas las redes 5G— e iniciativas políticas adecuadas a nivel de la UE.

Por último, la seguridad de las redes 5G reviste importancia estratégica para la Unión. La inversión extranjera en sectores estratégicos, la adquisición de activos, tecnologías e infraestructuras críticos en la Unión y el suministro de equipos críticos también pueden plantear riesgos para la seguridad de la Unión.

El nuevo **marco de la Unión para el control de las inversiones extranjeras directas**[41] entró en vigor el 10 de abril de 2019. Durante los próximos dieciocho meses, la Comisión y los Estados miembros tomarán las medidas necesarias para garantizar que la Unión pueda aplicar plenamente el Reglamento para el control de las inversiones a partir del 11 de octubre de 2020.

IV. LUCHA CONTRA EL BLANQUEO DE CAPITALES

La capacidad de delincuentes y terroristas de transferir fondos entre cuentas bancarias en cuestión de horas les permite preparar más fácilmente sus atentados terroristas o blanquear ilícitamente los productos del delito en los distintos Estados miembros. Para hacer frente a este reto, la Unión ha desarrollado un sólido **marco normativo para la lucha contra el blanqueo de capitales y la financiación del terrorismo**, en consonancia con las normas internacionales adoptadas por el Grupo de Acción Financiera Internacional.

Dada la necesidad de seguir el ritmo de la evolución de las tendencias, del desarrollo tecnológico y del ingenio adaptativo de los delincuentes para aprovechar cualquier laguna o ángulo muerto en el sistema, el 24 de julio de 2019 la Comisión adoptó un **paquete de cuatro informes** que analizan los riesgos y vulnerabilidades actuales relacionados con el blanqueo de capitales, y evalúan el modo en que los actores pertinentes aplican el marco tanto en el sector

[41] Reglamento (UE) 2019/452, de 19.3.2019, para el control de las inversiones extranjeras directas en la Unión. El nuevo marco crea un mecanismo de cooperación en el que los Estados miembros y la Comisión podrán intercambiar información y comunicar las dudas que les plantean determinadas inversiones específicas; Permitirá también a la Comisión emitir dictámenes cuando una inversión suponga una amenaza para la seguridad o el orden público de varios Estados miembros, o pueda socavar un proyecto o un programa de interés para el conjunto de la UE. El Estado miembro en el que se realiza la inversión tiene la última palabra sobre esta.

público como en el privado[42].

El paquete incluye una **evaluación de la posible interconexión de los registros nacionales centralizados de cuentas bancarias y los sistemas de recuperación de datos** en la UE. Estos sistemas centralizados nacionales permiten la identificación de cualquier persona física o jurídica que sea titular o controle cuentas de pagos, cuentas bancarias y cajas de seguridad, información que a menudo es crucial para las autoridades competentes en la lucha contra el blanqueo de capitales y la financiación del terrorismo. La 5.ª Directiva contra el blanqueo de capitales[43] exige a los Estados miembros que establezcan tales sistemas nacionales centralizados y que otorguen acceso directo a sus unidades de información financiera. Las normas recientemente adoptadas a fin de facilitar el uso de información financiera para combatir la delincuencia grave[44] prevén la creación de órganos encargados de hacer cumplir la ley especializados y de organismos de recuperación de activos con acceso directo a sus respectivos registros nacionales centralizados de cuentas bancarias. Partiendo de esta base, y tal como exige la Directiva contra el blanqueo de capitales, el informe evalúa varias soluciones informáticas a escala de la UE ya operativas o en fase de desarrollo, que pueden servir de modelo para una posible interconexión de los sistemas nacionales centralizados. Dado que una futura interconexión a escala de la UE de los mecanismos centralizados aceleraría el acceso a la información financiera y facilitaría la cooperación transfronteriza de las autoridades competentes, la Comisión tiene la intención de seguir consultando a las partes interesadas pertinentes, los gobiernos, las unidades de información financiera, los órganos encargados de hacer cumplir la ley y los organismos de recuperación de activos, como «usuarios finales» potenciales de un posible sistema de interconexión.

Como parte de la reflexión de la Comisión sobre el trabajo de las unidades de inteligencia financiera, un informe en el que se evalúa la **cooperación entre las unidades de inteligencia financiera** examina la cooperación tanto dentro de la Unión como con terceros países[45]. En él se señalan algunas deficiencias que es probable que sigan existiendo hasta que las tareas y las obligaciones de cooperación transfronteriza de las unidades de información financiera estén claramente definidas en el marco jurídico de la UE para la lucha contra el blanqueo de capitales y la financiación del terrorismo. La evaluación también pone de manifiesto la necesidad de un mecanismo más sólido para coordinar y apoyar la cooperación y el análisis transfronterizos.

---

42 Report on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities (Informe sobre la evaluación del riesgo de blanqueo de capitales y financiación del terrorismo en relación con el mercado interior y las actividades transfronterizas) [COM (2019) 370 final, de 24.7.2019], Report on the interconnection of national centralised automated mechanisms (central registries or central electronic data retrieval systems) of the Member States on bank accounts [Informe sobre la interconexión de mecanismos automatizados nacionales (registros centrales o sistemas centrales electrónicos de recuperación de datos) de los Estados miembros sobre las cuentas bancarias] (COM (2019) 372 final, de 24.7.2019), Report on the assessment of recent alleged money laundering cases involving EU credit institutions (Informe sobre la evaluación de los casos recientes de presunto blanqueo de capitales con participación de entidades de crédito de la UE) [COM (2019) 373 final, de 24.7.2019], Report assessing the framework for cooperation between Financial Intelligence Units (Informe de evaluación del marco de cooperación entre las Unidades de Información Financiera) [COM (2019) 371 final, de 24.7.2019].

43 Directiva (UE) 2015/849 de 20.5.2015.

44 Directiva (UE) 2019/1153 de 20.6.2019.

45 Esta evaluación viene exigida por el artículo 65, apartado 2, de la 5.ª Directiva contra el blanqueo de capitales [Directiva (UE) 2018/843 de 30.5.2018].

Más allá de los actuales esfuerzos por luchar contra el blanqueo de capitales y la financiación del terrorismo, y también en respuesta al llamamiento del Parlamento Europeo[46], la Comisión seguirá evaluando la necesidad, la viabilidad técnica y la proporcionalidad de medidas adicionales para rastrear la financiación del terrorismo en la UE[47].

V. EJECUCIÓN EN LO RELATIVO A OTRAS CUESTIONES DE SEGURIDAD PRIORITARIAS

1. Ejecución de las medidas legislativas en el marco de la Unión de la Seguridad

Ponerse de acuerdo sobre las medidas que se han de adoptar en el marco de la Unión de la Seguridad no implica el fin del proceso, pues resulta esencial garantizar que, posteriormente, los Estados miembros las ejecuten con celeridad y de forma integral a fin de aprovechar plenamente sus beneficios. A tal efecto, la Comisión está apoyando activamente a los Estados miembros, en particular concediéndoles financiación y facilitando el intercambio de buenas prácticas.
Cuando proceda, sin embargo, la Comisión está dispuesta a hacer pleno uso de las competencias que le confieren los Tratados para garantizar el cumplimiento de la legislación de la UE, lo que incluye, en su caso, la incoación de procedimientos de infracción.

El plazo para la aplicación de la **Directiva relativa al registro de nombres de pasajeros de la UE**[48] expiró el 25 de mayo de 2018. Hasta la fecha, 25 Estados miembros han notificado su plena transposición a la Comisión[49]. Dos Estados miembros aún no han llevado a cabo la plena transposición, a pesar de los procedimientos de infracción iniciados el 19 de julio de 2018[50]. En paralelo, la Comisión sigue apoyando a los Estados miembros en sus esfuerzos por completar el desarrollo de sus sistemas de registro de nombres de los pasajeros, en particular facilitando el intercambio de información y las buenas prácticas.

El plazo de transposición de la **Directiva sobre la lucha contra el terrorismo**[51] expiró el 8 de septiembre de 2018. Hasta la fecha, 22 Estados miembros han notificado su plena transposición a la Comisión. Tres Estados miembros siguen sin comunicar la adopción de legislación nacional que transponga plenamente la Directiva, a pesar de los procedimientos de infracción iniciados el 22 de noviembre de 2018[52].

El plazo para la transposición de la **Directiva sobre el control de la adquisición y tenencia de armas**[53] expiró el 14 de septiembre de 2018. Hasta la fecha, ocho Estados miembros han

---

46 En el informe final que aprobó en diciembre de 2018, la Comisión Especial sobre Terrorismo del Parlamento Europeo abogó por la creación de un sistema de la Unión Europea de seguimiento de la financiación del terrorismo centrado en las operaciones de personas vinculadas con el terrorismo y su financiación en la zona única de pagos en euros.

47 Véase el Decimoctavo informe de situación hacia una Unión de la Seguridad genuina y efectiva [COM (2019) 145 final, de 20.3.2019].

48 Directiva (UE) 2016/681 de 27.4.2016.

49 Las referencias a una notificación de transposición completa tienen en cuenta las declaraciones de los Estados miembros y se entienden sin perjuicio de la verificación de la transposición por parte de los servicios de la Comisión.

50 Eslovenia ha notificado la transposición parcial. España no ha notificado la transposición (situación a 24 de julio de 2019).

51 Directiva (UE) 2017/541 de 15.3.2017.

52 Polonia ha notificado la transposición parcial. Grecia y Luxemburgo no han notificado transposición alguna (situación a miércoles, 24 de julio de 2019).

53 Directiva (UE) 2017/853 de 17.5.2017.

notificado su plena transposición a la Comisión. Veinte Estados miembros siguen sin comunicar la adopción de medidas nacionales que transpongan plenamente la Directiva, a pesar de los procedimientos de infracción iniciados el 22 de noviembre de 2018[54].

Con respecto a la transposición al Derecho nacional de la **Directiva sobre protección de datos en el ámbito penal**[55], el plazo para la transposición expiró el 6 de mayo de 2018. Hasta la fecha, veinte Estados miembros han notificado su plena transposición a la Comisión[56]. Siete Estados miembros siguen sin comunicar la adopción de medidas nacionales que transpongan plenamente la Directiva, a pesar de los procedimientos de infracción incoados por la Comisión el 19 de julio de 2018[57].

Los Estados miembros tenían de plazo hasta el 9 de mayo de 2018 para transponer la **Directiva relativa a la seguridad de las redes y sistemas de información**[58] al Derecho nacional. Hasta la fecha, veintiséis Estados miembros han notificado la plena transposición a la Comisión y dos Estados miembros han transpuesto parcialmente la Directiva[59]. Además, a más tardar el 9 de noviembre de 2018, los Estados miembros estaban obligados a identificar a los operadores de servicios esenciales en consonancia con la Directiva. Antes del 9 de mayo de 2019, la Comisión debía presentar al Parlamento Europeo y al Consejo un informe de evaluación de la coherencia del enfoque en la identificación de los operadores de servicios esenciales identificados en su territorio. No obstante, dado que algunos Estados miembros aún no habían facilitado información completa sobre el proceso de identificación, la Comisión ha tenido que retrasar la presentación de su informe.

La Comisión está evaluando la transposición de la **cuarta Directiva antiblanqueo**[60], al mismo tiempo que trabaja para comprobar que los Estados miembros ejecutan las normas. La Comisión ha incoado procedimientos de infracción contra veinticuatro Estados miembros, pues considera que las comunicaciones que le han remitido no garantizan la transposición plena de la Directiva[61].

La Comisión insta a los Estados miembros a que, con carácter de urgencia, adopten las medidas necesarias para incorporar plenamente las siguientes Directivas a su ordenamiento jurídico y le comuniquen las medidas correspondientes:

54 Bélgica, Chequia, Estonia, Lituania, Polonia, Portugal, Suecia y Reino Unido han notificado la transposición parcial. Alemania, Irlanda, Grecia, España, Chipre, Luxemburgo, Hungría, Países Bajos, Rumanía, Eslovenia, Eslovaquia y Finlandia no han notificado la transposición (situación a 24 de julio de 2019).

55 Directiva (UE) 2016/680 de 27.4.2016.

56 Veinte Estados miembros han completado la transposición (situación a 24 de julio de 2019).

57 Letonia, Portugal, Eslovenia y Finlandia han notificado la transposición parcial. Grecia y España no han notificado transposición alguna. Aunque Alemania ha notificado la transposición completa, la Comisión considera que esta transposición no está completa (situación a 24 de julio de 2019).

58 Directiva (UE) 2016/1148 de 27.4.2016.

59 Bélgica y Hungría han transpuesto parcialmente la Directiva (situación a 24 de julio de 2019).

60 Directiva (UE) 2015/849 de 20.5.2015.

61 Bélgica, Bulgaria, Chequia, Dinamarca, Alemania, Estonia, Irlanda, España, Francia, Italia, Chipre, Letonia, Lituania, Hungría, Países Bajos, Austria, Polonia, Portugal, Rumanía, Eslovenia, Eslovaquia, Finlandia, Suecia y Reino Unido (situación a 24 de julio de 2019).

- **Directiva de la UE relativa al registro de los nombres de los pasajeros**, en relación con la cual un Estado miembro aún no ha notificado su incorporación al ordenamiento jurídico nacional y otro Estado miembro debe completar aún la notificación de la transposición[62];
- **Directiva relativa a la lucha contra el terrorismo**, en relación con la cual dos Estados miembros aún no han notificado su incorporación al ordenamiento jurídico nacional y un Estado miembro debe completar la notificación sobre su transposición[63];
- **Directiva sobre el control de la adquisición y tenencia de armas**, en relación con la cual doce Estados miembros aún no han notificado su incorporación al ordenamiento jurídico nacional y otros ocho deben completar la notificación sobre su transposición[64];
- **Directiva sobre protección de datos en el ámbito penal**, en relación con la cual dos Estados miembros aún no han notificado su transposición al ordenamiento jurídico nacional y otros cinco deben completar la notificación sobre su transposición[65];
- **Directiva relativa a la seguridad de las redes y sistemas de información**, respecto de la cual dos Estados miembros aún deben completar la notificación de la transposición[66]; y
- **cuarta Directiva contra el blanqueo de capitales**, en relación con la cual veinticuatro Estados miembros deben completar aún la notificación de la transposición[67].

2. Contrarrestar la desinformación y proteger las elecciones frente a otras amenazas facilitadas por la cibernética

La protección de las instituciones y procesos democráticos frente a la desinformación y las interferencias conexas constituye un importante reto para las sociedades de todo el mundo. Con el objeto de hacer frente a este desafío, la UE ha creado una **sólido marco para la acción coordinada contra la desinformación** que respeta plenamente los valores y derechos fundamentales europeos[68]. Según lo establecido en la Comunicación conjunta de 14 de junio de 2019 sobre la ejecución del Plan de Acción contra la Desinformación[69], los trabajos sobre varias líneas complementarias han ayudado a reducir los espacios aprovechados para la desinformación y a preservar la integridad de las elecciones al Parlamento Europeo.

En sus conclusiones de 21 de junio de 2019[70], el Consejo Europeo acogió favorablemente la intención de la Comisión de llevar a cabo una evaluación exhaustiva de la ejecución de los

62 Eslovenia ha notificado la transposición parcial. España no ha notificado la transposición (situación a 24 de julio de 2019).

63 Polonia ha notificado la transposición parcial. Grecia y Luxemburgo no han notificado transposición alguna (situación a 24 de julio de 2019).

64 Bélgica, Chequia, Estonia, Lituania, Polonia, Portugal, Suecia y Reino Unido han notificado la transposición parcial. Alemania, Irlanda, Grecia, España, Chipre, Luxemburgo, Hungría, Países Bajos, Rumanía, Eslovenia, Eslovaquia y Finlandia no han notificado la transposición (situación a 24 de julio de 2019).

65 Letonia, Portugal, Eslovenia y Finlandia han notificado la transposición parcial. Grecia y España no han notificado transposición alguna. Aunque Alemania ha notificado la transposición completa, la Comisión considera que esta transposición no está completa (situación a 24 de julio de 2019).

66 Bélgica y Hungría han transpuesto parcialmente la Directiva (situación a 24 de julio de 2019).

67 Bélgica, Bulgaria, Chequia, Dinamarca, Alemania, Estonia, Irlanda, España, Francia, Italia, Chipre, Letonia, Lituania, Hungría, Países Bajos, Austria, Polonia, Portugal, Rumanía, Eslovenia, Eslovaquia, Finlandia, Suecia y Reino Unido (situación a 24 de julio de 2019).

68 Véase el Plan de Acción contra la Desinformación [JOIN(2018) 36 final, de 5.12.2018].

69 JOIN(2019) 12 final, de 14.6.2019.

70 https://www.consilium.europa.eu/media/39922/20-21-euco-final-conclusions-en.pdf. La convocatoria del Consejo Europeo se basa en las aportaciones de la Presidencia rumana del Consejo, así como de la Comisión y de la alta representante para Asuntos Exteriores y Política de Seguridad sobre las lecciones

compromisos asumidos por las plataformas en línea y otros firmantes del **Código de Buenas Prácticas contra la Desinformación**[71] e invitó a la Comisión y a la alta representante de la Unión para Asuntos Exteriores y Política de Seguridad a evaluar de forma permanente la «naturaleza cambiante de las amenazas y el riesgo creciente de injerencias malintencionadas y de manipulación en línea asociadas al desarrollo de la inteligencia artificial y las técnicas de recopilación de datos» y responder adecuadamente.

La Comisión y el alto representante llevarán adelante sus trabajos en este ámbito en consonancia con las conclusiones del Consejo Europeo. En marzo de 2019, la Comisión y la alta representante crearon un **sistema de alerta temprana** entre las instituciones de la UE y los Estados miembros para facilitar el intercambio de información sobre las campañas de desinformación y coordinar las respuestas. La primera reunión de los puntos de contacto de los Estados miembros tras las elecciones al Parlamento Europeo tuvo lugar en Tallin del 3 al 4 de junio de 2019. Para reforzar aún más el sistema de alerta temprana, la alta representante y la Comisión, en estrecha cooperación con los Estados miembros, revisará el funcionamiento del sistema de alerta temprana en otoño de 2019. También desarrollarán una metodología común para el análisis y el desenmascaramiento de las campañas de desinformación, así como unas relaciones asociativas más fuertes con socios internacionales como el G7 y la OTAN.

También prosiguen los trabajos en la **Red Europea de Cooperación en materia de Elecciones**[72], que celebró su primera reunión el 7 de junio de 2019 para hacer balance de las elecciones al Parlamento Europeo. Estas reflexiones y otras aportaciones de las autoridades nacionales, los partidos políticos y las plataformas en línea pertinentes contribuirán al informe general de la Comisión sobre las elecciones al Parlamento Europeo que se adoptará en octubre de 2019. Los Estados miembros han recurrido a la red en relación con elecciones distintas de las del Parlamento Europeo, lo que pone de manifiesto su utilidad general para garantizar la integridad de la democracia en la UE.

La Comisión también seguirá supervisando y promoviendo la puesta en práctica de los compromisos asumidos por las plataformas en el **Código de Buenas Prácticas en materia de Desinformación**.
Los informes presentados por Google, Twitter y Facebook con arreglo al Código de Buenas Prácticas muestran que todas las plataformas tomaron medidas con anterioridad a las elecciones al Parlamento Europeo mediante el etiquetado de los anuncios políticos y haciendo que estos fuesen públicamente accesibles mediante bibliotecas de publicidad política que

---

aprendidas con respecto a la desinformación y la garantía de elecciones libres y justas, incluida la Comunicación Conjunta sobre la Ejecución del Plan de Acción contra la Desinformación.

71 El Código de Buenas Prácticas fue firmado por las plataformas en línea Facebook, Google y Twitter, Mozilla, y por los anunciantes y la industria publicitaria en octubre de 2018, y establece normas de autorregulación para luchar contra la desinformación. El Código pretende alcanzar los objetivos establecidos en la Comunicación de la Comisión de abril de 2018 sobre la lucha contra la desinformación en línea (COM/2018/236 final, de 26.4.2018), estableciendo una amplia gama de compromisos, desde la transparencia en la publicidad política hasta el cierre de cuentas falsas y la desmonetización de los vectores de desinformación.

72 La Red Europea de Cooperación en materia de Elecciones reúne los puntos de contacto de las redes nacionales de cooperación electoral, compuestas por las autoridades competentes en materia electoral y las autoridades responsables de supervisar y hacer cumplir las normas relacionadas con las actividades en línea que puedan incidir en los contextos electorales. La Red Europea de Cooperación en materia de Elecciones sirve para alertar de las amenazas, intercambiar mejores prácticas entre las redes nacionales, debatir sobre soluciones comunes para los retos detectados y fomentar proyectos y ejercicios comunes entre las redes nacionales.

permitían la realización de búsquedas. Al mismo tiempo, existe un margen de mejora que ha sido señalado por el Grupo de Entidades Reguladoras Europeas para los Servicios de Comunicación Audiovisual[73]. En particular, sigue existiendo una falta de acceso a los datos en bruto detallados necesarios para un control exhaustivo. Por último, las plataformas deben ofrecer a la comunidad investigadora un acceso significativo a los datos, en consonancia con las normas de protección de datos personales. Antes de que acabe el año, la Comisión llevará a cabo una evaluación exhaustiva del cumplimiento de todos los compromisos contraídos en virtud del Código de Buenas Prácticas durante su período inicial de 12 meses. Sobre esta base, la Comisión puede estudiar otras medidas, en particular de carácter normativo, para mejorar la respuesta a largo plazo de la UE a la desinformación.

3. Preparación y protección

El fortalecimiento de las defensas y el incremento de la resiliencia frente a las amenazas para la seguridad es un aspecto importante del trabajo en pos de una Unión de la Seguridad genuina y efectiva. Este trabajo incluye el apoyo que presta la Comisión a los Estados miembros y a sus autoridades locales para reforzar la **protección de los espacios públicos**[74] y el apoyo a los Estados miembros con vistas a mejorar la preparación frente a los **riesgos de seguridad químicos, biológicos, radiológicos y nucleares**[75] mediante la ejecución de los dos planes de acción para este ámbito y el análisis de las necesidades relativas a las capacidades de reacción correspondientes que se han de desarrollar en el marco del rescEU[76]. Por lo que se refiere a la evolución de las amenazas químicas[77], la Comisión ha elaborado, en cooperación con los Estados miembros y tras consultar a sus socios internacionales, una lista de los productos químicos más preocupantes en términos de uso indebido con fines terroristas. La lista de la UE sirve de base para seguir trabajando con el fin de reducir la accesibilidad de estos productos químicos y para trabajar con los fabricantes en la mejora de las capacidades de detección.

---

73 El Grupo de Entidades Reguladoras Europeas para los Servicios de Comunicación Audiovisual reúne a los directores o altos representantes de organismos reguladores nacionales independientes en el ámbito de los servicios audiovisuales para asesorar a la Comisión sobre la ejecución de la Directiva de servicios de comunicación audiovisual de la UE (Directiva 2010/13/UE de 10.3.2010). En su última reunión, celebrada los días 20 y 21 de junio de 2019 en Bratislava, el Grupo presentó los resultados del trabajo realizado hasta la fecha sobre la desinformación, centrándose en las elecciones al Parlamento Europeo de 2019 y en los ámbitos conexos de la publicidad política y temática.

74 Véanse las «Buenas prácticas para que las autoridades públicas y los operadores privados refuercen la seguridad de los espacios públicos», tal como se establecen en el «Decimoctavo informe sobre la evolución hacia una Unión de la Seguridad genuina y efectiva» [COM (2019) 145 final, de 20.3.2019]. Esto se basa en el «Plan de acción para contribuir a la protección de los espacios públicos» de octubre de 2017 [COM (2017) 612 final, de 18.10.2017]. El 5 de junio de 2019 se celebró la tercera reunión del Foro de Operadores del Foro de la UE sobre la protección de los espacios públicos. Esta reunión congregó a representantes de los Estados miembros de la UE y de operadores privados de espacios públicos, representados a través de 14 asociaciones europeas que abarcan los sectores de la hostelería, las actuaciones en directo, los espectáculos musicales y de entretenimiento, los parques de atracciones, la aviación, el transporte ferroviario, los centros comerciales y las telecomunicaciones, los servicios de seguridad privada y los fabricantes de equipos de seguridad.

75 En particular mediante la ejecución del «Plan de acción para mejorar la preparación ante los riesgos de seguridad químicos, biológicos, radiológicos y nucleares» de octubre de 2017 [COM (2017) 610 final, de 18.10.2017].

76 Véase el artículo 12, apartado 2, de la Decisión n.º 1313/2013/UE, relativa a un Mecanismo de Protección Civil de la Unión (17.12.2013), modificada por la Decisión (UE) 2019/420 (13.3.2019).

77 Véanse las medidas reforzadas contra las amenazas químicas que figuran en el Decimoquinto Informe sobre la evolución hacia una Unión de la Seguridad genuina y efectiva [COM (2018) 470 final, de 13.6.2018].

Las tecnologías de las aeronaves no tripuladas permiten realizar una amplia gama de operaciones. Dada su rápida expansión en los últimos años en el mercado de sistemas de aeronaves no tripuladas para fines militares, comerciales civiles y de ocio, los **drones** representan, al mismo tiempo, una oportunidad y una amenaza cada vez mayor para las infraestructuras críticas (incluida la aviación), los espacios y los actos públicos, y los lugares e individuos vulnerables. En Europa, se han utilizado drones para perturbar operaciones de aviación y de aplicación de la ley, escudriñar infraestructuras críticas e introducir contrabando en las cárceles y a través de las fronteras.

La Comisión apoya a los Estados miembros en la lucha contra la amenaza creciente que representan los drones para los ciudadanos y las funciones sociales básicas, sin descartar por ello sus usos beneficiosos, por ejemplo en operaciones de respuesta a emergencias. La Comisión ha adoptado recientemente **normas comunes a escala de la UE sobre el funcionamiento seguro de los drones**[78] a fin de mitigar el riesgo de uso malintencionado, entre las que figuran disposiciones que exigen el registro de los operadores y que permiten la identificación remota. Por otra parte, la Comisión apoya a los Estados miembros a través del seguimiento de las tendencias en la evolución de la amenaza que suponen los drones, financiando proyectos de investigación pertinentes y medidas de desarrollo de las capacidades y facilitando el intercambio entre los Estados miembros y otras partes interesadas. Con el fin de intensificar este apoyo, la Comisión organizará, el 17 de octubre de 2019, una conferencia internacional de alto nivel para hacer frente a los riesgos planteados por los drones.

En respuesta a la necesidad de adoptar una visión amplia sobre la política de la UE en materia de **protección de infraestructuras críticas**[79], el 23 de julio de 2019 la Comisión presentó una evaluación de la **Directiva sobre infraestructuras críticas europeas**[80] como marco jurídico para la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección. La evaluación puso de manifiesto que el contexto en el que operan las infraestructuras críticas en Europa ha cambiado considerablemente desde la entrada en vigor de la Directiva, en particular debido a la evolución legislativa en sectores especialmente afectados por la Directiva, como el de la energía[81], y que, a consecuencia de esta modificación de las circunstancias, las disposiciones de la Directiva solo conservan una pertinencia parcial. Al mismo tiempo, los Estados miembros siguen apoyando las políticas de la UE de protección de infraestructuras críticas que respetan la subsidiariedad y aportan valor añadido.

4. Dimensión exterior

Habida cuenta de la naturaleza transfronteriza y mundial de la mayoría de las amenazas para la seguridad a las que se enfrenta nuestra Unión, la cooperación con organizaciones internacionales y países socios de fuera de la UE forma parte integrante del trabajo hacia una

---

78 Reglamento de Ejecución (UE) 2019/947 de la Comisión, de 24 de mayo de 2019, relativo a las normas y los procedimientos aplicables a la utilización de aeronaves no tripuladas (DO L 152 de 11.6.2019).

79 La Evaluación Exhaustiva de la Política de Seguridad de la UE de 2017 [SWD (2017) 278 final, de 26.7.2017] señaló la necesidad de adoptar una visión amplia sobre la política de protección de infraestructuras críticas de la UE.

80 La Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección, tiene por objetivo reforzar la protección de las infraestructuras críticas en la Unión Europea.

81 En particular, el Reglamento (UE) 2017/1938, de 25.10.2017, sobre medidas para garantizar la seguridad del suministro de gas, y el Reglamento (UE) 2019/941, de 5.6.2019, sobre la preparación frente a los riesgos en el sector de la electricidad.

Unión de la Seguridad genuina y efectiva.

El aprovechamiento de los beneficios de la cooperación multilateral forma parte integrante de este esfuerzo, e incluye la cooperación entre la UE y las Naciones Unidas, reforzada recientemente con la firma del **marco de lucha contra el terrorismo entre las Naciones Unidas y la UE** en Nueva York el 24 de abril de 2019, con ocasión del segundo diálogo político de alto nivel entre las Naciones Unidas y la UE en materia de lucha contra el terrorismo[82]. El marco promueve la cooperación en materia de desarrollo de capacidades para luchar contra el terrorismo y prevenir y contrarrestar el extremismo violento en África, Oriente Medio y Asia; asimismo, establece los ámbitos de cooperación entre las Naciones Unidas y la UE y las prioridades hasta 2020.

La **cooperación en materia de seguridad con los Balcanes Occidentales** constituye una prioridad regional particular y conlleva la aplicación de una serie de medidas prioritarias relacionadas con la seguridad, indicadas en la Estrategia sobre los Balcanes Occidentales de 2018[83]. A tal fin, el 4 de abril de 2019 la Comisión organizó la primera reunión del Grupo de Trabajo Interinstitucional para los Balcanes Occidentales, en la que representantes de siete agencias de la UE informaron sobre sus experiencias e intensificaron la cooperación operativa con sus socios de la región, en particular en lo relativo a la lucha contra la delincuencia organizada, el terrorismo, las armas de fuego, las drogas, el tráfico ilícito de migrantes y la trata de seres humanos. Se han iniciado, en colaboración con los seis países de los Balcanes Occidentales, encuestas sobre riesgos híbridos. Otro ejemplo tangible de cooperación con la región es el Acuerdo sobre el Estatuto de la Guardia Europea de Fronteras y Costas entre la UE y Albania, que entró en vigor el 1 de mayo de 2019 y que fue seguido poco después por el despliegue de equipos de la Agencia Europea de la Guardia de Fronteras y Costas en la frontera con Grecia. Esta es la primera vez que se celebra un acuerdo de este tipo con un tercer país y se destinan efectivos al mismo. Se espera que, en breve, se firmen acuerdos similares con otros países de la región.

Además, en julio de 2019 se destinó a Albania un funcionario de enlace de Europol para seguir ayudando a las autoridades albanesas en sus esfuerzos por prevenir y luchar contra la delincuencia organizada. A fin de intensificar la lucha contra el tráfico de armas de fuego, la Comisión presentó, el 27 de junio de 2019, una evaluación del Plan de Acción 2015-2019 para la **lucha contra el tráfico de armas de fuego** entre la UE y la región sudoriental de Europa[84]. La evaluación demuestra el valor añadido de la cooperación, pero destaca que siguen siendo necesarios esfuerzos adicionales mediante, por ejemplo, la creación de centros nacionales de coordinación en materia de armas de fuego eficaces o la armonización de la recogida de información y la elaboración de informes sobre las incautaciones de armas de fuego.

La UE considera igualmente prioritario el desarrollo de la **cooperación con los países de Oriente Medio y el norte de África** en el ámbito de la seguridad. La UE ha puesto en marcha un diálogo en materia de seguridad con Túnez y Argelia. La UE y Túnez celebraron el Tercer Diálogo sobre Seguridad y Lucha contra el Terrorismo el 12 de junio en Túnez, mientras que el Segundo Diálogo entre la UE y Argelia sobre Seguridad y Lucha contra el Terrorismo tuvo

82 https://eeas.europa.eu/sites/eeas/files/2019042019_un-eu_framework_on_counter-terrorism.pdf

83 COM(2018) 65 final de 6.2.2018.

84 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20190627_com-2019-293-commission-report_es.pdf

lugar el 12 de noviembre de 2018 en Argel. Se están manteniendo conversaciones para iniciar un diálogo estructurado sobre seguridad con Marruecos a raíz del reciente Consejo de Asociación celebrado el 27 de junio, en el que la UE y Marruecos reconocieron la importancia de incrementar la cooperación en materia de seguridad para hacer frente a los retos comunes. Paralelamente, se están manteniendo conversaciones para desarrollar un diálogo estructurado sobre seguridad con Egipto, tal como se ha vuelto a confirmar en la última reunión de altos funcionarios de la UE y Egipto celebrada el 10 de julio en El Cairo.

Sobre la base del mandato del Consejo, la Comisión ha iniciado conversaciones informales con la mayoría de los países de **Oriente Próximo y el norte de África** con vistas a entablar negociaciones oficiales para la celebración de un acuerdo internacional sobre el intercambio de datos personales entre la Agencia de la Unión Europea para la Cooperación Policial (**Europol**) y las autoridades competentes de los países de **Oriente Próximo y el norte de África** en materia de lucha contra la delincuencia grave y el terrorismo. En este contexto, la Comisión está promoviendo también la celebración directa de acuerdos de trabajo entre Europol y las autoridades asociadas en los países de **Oriente Medio y el norte de África** con el fin de facilitar un marco formal para la cooperación continua en el plano estratégico.

La UE y los **Estados Unidos** son socios cercanos y estratégicos a la hora de hacer frente a las amenazas comunes y reforzar la seguridad. En su reunión ministerial de Justicia y Asuntos de Interior de 19 de junio de 2019, la UE y los Estados Unidos reiteraron que la lucha contra el terrorismo figura entre sus máximas prioridades. Por lo que respecta al Acuerdo UE-EE.UU. sobre el registro de nombres de los pasajeros[85], ambas partes volvieron a insistir en su importancia y se comprometieron a iniciar una evaluación conjunta en septiembre de 2019 para evaluar su puesta en práctica, de conformidad con las disposiciones del Acuerdo. Asimismo, ambas partes se comprometieron a intensificar sus esfuerzos conjuntos en la lucha contra el terrorismo, en particular mediante un mayor intercambio de la información recopilada en zonas de combate para su uso en investigaciones y procesos penales.

A fin de intensificar esta cooperación, la Comisión, junto con el coordinador de la UE para la lucha contra el terrorismo, organizó un taller de alto nivel sobre información del campo de batalla el 10 de julio de 2019 en Bruselas. Este taller reunió a altos funcionarios de los Ministerios de Defensa, Interior y Justicia de los Estados miembros, de los Estados Unidos, de Europol y de Eurojust, así como a representantes de organizaciones internacionales para intercambiar puntos de vista sobre el uso de la información del campo de batalla y reflexionar juntos sobre los desafíos procesales, jurídicos y operativos a los que se enfrentan en la actualidad a la hora de identificar a los terroristas y llevarlos ante la justicia. Asimismo, la UE y los Estados Unidos mantuvieron en Bruselas un «Diálogo para el desarrollo de capacidades en materia química, biológica, radiológica y nuclear» el 14 y 15 de mayo de 2019, con el fin de coordinar sus esfuerzos para reducir la amenaza que representan las armas de destrucción masiva e incrementar la seguridad QBRN a escala mundial.

El **Acuerdo sobre el Programa de Seguimiento de la Financiación del Terrorismo entre la UE y los Estados Unidos**[86] está en vigor desde 2010 y regula la transmisión y el tratamiento de datos para identificar, rastrear y perseguir a terroristas y sus redes. El Acuerdo contiene garantías que aseguran la protección de los datos de los ciudadanos de la UE y prevé

[85] DO L 215 de 11.8.2012, p. 5.
[86] DO L 195 de 27.7. 2010, p. 5).

una revisión periódica de «las salvaguardias, los controles y las disposiciones en materia de reciprocidad». En un informe periódico de evaluación[87] publicado el 22 de julio de 2019, la Comisión señaló que está convencida de que el Acuerdo, incluidas sus salvaguardias y controles esenciales, se está aplicando correctamente. Acoge con satisfacción la transparencia constante de las autoridades estadounidenses en el intercambio de información, que pone de manifiesto el valor del Programa de Seguimiento de la Financiación del Terrorismo en nuestros esfuerzos conjuntos en materia de lucha contra el terrorismo. La información facilitada con arreglo al Acuerdo ha sido fundamental para avanzar en investigaciones específicas relacionadas con atentados terroristas en territorio europeo, incluidos los atentados en Estocolmo, Barcelona y Turku en 2017. Los Estados miembros y Europol han incrementado su utilización del mecanismo, y los datos del Programa de Seguimiento de la Financiación del Terrorismo han generado una cantidad siete veces mayor de pistas de investigación que en el período de referencia anterior. Se espera que la próxima revisión conjunta del acuerdo tenga lugar en 2021.

Por lo que respecta a la cooperación internacional en materia de intercambio de **registros de nombres de pasajeros a efectos de la lucha contra el terrorismo y la delincuencia grave**, en la 17.ª Cumbre UE-Canadá, celebrada en Montreal los días 17 y 18 de julio de 2019, la UE y Canadá se congratularon de haber concluido las negociaciones para un nuevo Acuerdo sobre el Registro de Nombres de los Pasajeros. Si bien Canadá ha advertido sobre su obligación de proceder a un control de la legalidad, las partes se comprometen, bajo reserva de los resultados que arroje dicho control, a ultimar el Acuerdo lo antes posible, reconociendo el papel fundamental de este tanto a la hora de incrementar la seguridad como de garantizar la privacidad y la protección de los datos personales. Por lo que se refiere al Acuerdo sobre el Registro de Nombres de los Pasajeros[88] vigente entre la UE y Australia, la visita de un equipo de la UE a Canberra se celebrará en agosto de 2019 en el contexto de la revisión conjunta y la evaluación conjunta del Acuerdo.

La Comisión también está trabajando con los Estados miembros en el Consejo con vistas a la adopción de la posición de la UE a efectos del 40.º período de sesiones de la Asamblea de la **Organización de Aviación Civil Internacional**, que se celebrará del 24 de septiembre al 4 de octubre de 2019. La Asamblea fijará una dirección política y dará instrucciones al Consejo de la Organización de Aviación Civil Internacional acerca de los trabajos técnicos sobre los estándares de la Organización de Aviación Civil Internacional para el tratamiento de datos del registro de nombres de los pasajeros. El Consejo ha refrendado un documento informativo preparado por la Comisión en el que se resume la posición de la Unión sobre los principios fundamentales en que debe basarse cualquier norma futura relativa a un registro de nombres de pasajeros mundial. El documento informativo se presentará ante el organismo para conocimiento de aquellos de sus miembros que no forman parte de la UE.

VI. CONCLUSIÓN

Gracias a una estrecha cooperación entre el Parlamento Europeo, el Consejo, los Estados miembros y la Comisión, en los últimos años la UE ha avanzado considerablemente en el trabajo conjunto hacia una Unión de la Seguridad genuina y efectiva, acordando una serie de iniciativas legislativas prioritarias. Los Estados miembros, con el apoyo de la Comisión, están aplicando también una serie de medidas operativas no legislativas para reforzar la seguridad

[87] COM(2019) 342 final de 22.7.2019.
[88] DO L 186 de 14.7.2012, p. 4.

de todos los ciudadanos. Al mismo tiempo, hay todavía una serie de iniciativas prioritarias pendientes de la Unión de la Seguridad que requieren la adopción de medidas adicionales por parte de los colegisladores para hacer frente a amenazas inmediatas. La Comisión pide al Parlamento Europeo y al Consejo que adopten las medidas necesarias para alcanzar con celeridad un acuerdo sobre las propuestas legislativas destinadas a luchar contra la propaganda terrorista y la radicalización en línea, reforzar la ciberseguridad, facilitar el acceso a las pruebas electrónicas y completar el trabajo de implantación de sistemas de información más sólidos e inteligentes para la gestión de la seguridad, las fronteras y la migración.

La Comisión insta a los Estados miembros a que apliquen sin dilación e íntegramente toda la legislación adoptada en relación con la Unión de la Seguridad a fin de sacar partido a esta plenamente. Por otra parte, la Comisión pide a los Estados miembros que prosigan e intensifiquen el crucial trabajo relativo a las medidas prácticas destinadas a mejorar la seguridad de las infraestructuras digitales, contrarrestar la desinformación y otras amenazas facilitadas por la cibernética, intensificar la preparación y la protección, y reforzar la cooperación con socios de fuera de la Unión contra las amenazas compartidas. Tomadas en su conjunto, estas medidas aumentan la seguridad de todos los ciudadanos.