Consejo de la
Unión Europea

Bruselas, 31 de octubre de 2019
(OR. en)

13682/19

JAI 1139
COSI 220
FRONT 299
ASIM 131
DAPIX 321
ENFOPOL 471
SIRIS 161
VISA 231
FAUXDOC 72
COPEN 417
CYBER 295
DATAPROTECT 265
CT 113
JAIEX 161
EF 319

NOTA DE TRANSMISIÓN

De:	secretario general de la Comisión Europea, firmado por D. Jordi AYET PUIGARNAU, director
Fecha de recepción:	31 de octubre de 2019
A:	D. Jeppe TRANHOLM-MIKKELSEN, secretario general del Consejo de la Unión Europea
N.° doc. Ción.:	COM(2019) 552 final
Asunto:	COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, EL CONSEJO EUROPEO Y EL CONSEJO Vigésimo informe de situación relativo a una Unión de la Seguridad genuina y efectiva

Adjunto se remite a las Delegaciones el documento – COM(2019) 552 final.

Adj.: COM(2019) 552 final

COMISIÓN
EUROPEA

Bruselas, 30.10.2019
COM(2019) 552 final

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

Vigésimo informe de situación relativo a una Unión de la Seguridad genuina y efectiva

I. INTRODUCCIÓN

Este es el vigésimo informe sobre los progresos realizados en la construcción de una Unión de la Seguridad genuina y efectiva, cuyo objeto es la evolución registrada en dos pilares principales: la lucha contra el terrorismo y la delincuencia organizada y los medios que les prestan apoyo, y el refuerzo de nuestras defensas y de la resiliencia frente a esas amenazas.

Desde su primer día de mandato, la Comisión Juncker otorgó la máxima prioridad a la seguridad. Sobre la base de la Agenda Europea de Seguridad de abril de 2015[1] y de la Comunicación «Allanar el camino hacia una Unión de la Seguridad genuina y efectiva» de abril de 2016[2], la UE ha respondido con un enfoque coordinado a una serie de atentados terroristas y otros desafíos crecientes en materia de seguridad, haciendo progresos significativos en la mejora de nuestra seguridad colectiva[3]. Cada vez es más evidente que los retos actuales en materia de seguridad - ya se trate del terrorismo, la delincuencia organizada, los ciberataques, la desinformación u otras amenazas cibernéticas evolutivas - constituyen amenazas comunes. Solo trabajando juntos podremos alcanzar el nivel de seguridad colectiva que los ciudadanos demandan y esperan. En este entendimiento común se han fundado los progresos realizados hacia una Unión de la Seguridad genuina y efectiva. Guiado por las necesidades de las autoridades nacionales que trabajan para mantener la seguridad de los ciudadanos, el apoyo de la UE se ha centrado en aquellas medidas legislativas y operativas en las que una actuación conjunta puede repercutir en la seguridad de los Estados miembros. Este trabajo se ha llevado a cabo en estrecha colaboración con el Parlamento Europeo y el Consejo, y con total transparencia para el público en general. El pleno respeto de los derechos fundamentales ha sido el principio rector de esta labor, ya que la seguridad de la Unión solo puede garantizarse cuando los ciudadanos confían en que se respetan plenamente sus derechos fundamentales.

La UE ha trabajado en la **lucha contra el terrorismo** mediante la restricción del perímetro de actuación de los terroristas, con nuevas normas que dificultan su acceso a explosivos, armas de fuego y financiación, así como restringen sus movimientos. La UE ha intensificado el **intercambio de información** para proporcionar a las personas que trabajan en primera línea, los agentes de policía y los guardias de fronteras, un acceso eficiente a datos exactos y completos, haciendo el mejor uso posible de la información existente, colmando las lagunas de información y eliminando los ángulos muertos. La firme protección de las fronteras exteriores representa una condición previa de la seguridad en el espacio de libre circulación sin controles en las fronteras interiores. En marzo de 2019, el Parlamento Europeo y el Consejo alcanzaron un acuerdo sobre una **Guardia Europea de Fronteras y Costas** reforzada y totalmente equipada, y se espera que el nuevo Reglamento entre en vigor a principios de diciembre de 2019. La UE ha proporcionado una plataforma y financiación a quienes trabajan en las comunidades locales para intercambiar las mejores prácticas en materia de **lucha contra la radicalización y prevención del extremismo violento**, así como ha propuesto nuevas normas para eliminar efectivamente los contenidos terroristas en línea. El apoyo de la UE ha contribuido a que las **ciudades sean más resilientes** frente a los ataques, con planes de acción que respaldan la protección de los espacios públicos y mejoran la preparación ante los riesgos de seguridad químicos, biológicos, radiológicos y nucleares. La

[1] COM (2015) 185 final de 28.4.2015.
[2] COM (2016) 230 final de 20.4.2016.
[3] Para anteriores informes sobre la evolución hacia una Unión de la Seguridad genuina y efectiva, véase: https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security/legislative-documents_en.

UE ha afrontado las **amenazas cibernéticas y a la ciberseguridad** mediante la puesta en marcha de una nueva estrategia de ciberseguridad de la UE y la adopción de la legislación pertinente, y ha asumido la lucha contra la **desinformación** para mejorar la protección de nuestras elecciones. Se sigue trabajando para aumentar la seguridad de nuestra **infraestructura crítica digital**, incluida una cooperación reforzada para la **ciberseguridad de las redes 5G** en toda Europa.

Aún queda mucho por hacer. El ataque retransmitido en directo contra una sinagoga y el asesinato de dos ciudadanos en Halle, Alemania, el 9 de octubre de 2019, fueron un terrible recordatorio de la amenaza que supone el extremismo violento de derechas y el antisemitismo. También puso una vez más de manifiesto el uso indebido de Internet para la propaganda terrorista y, por tanto, la **necesidad de normas a escala de la UE para la supresión de contenidos terroristas en línea**. Los días 7 y 8 de octubre de 2019, el Consejo de Justicia y Asuntos de Interior debatió sobre la extrema derecha, el extremismo violento y el terrorismo, subrayando la necesidad de seguir trabajando, en particular en la lucha contra la propagación de los contenidos extremistas de derechas, tanto en línea como fuera de línea. Al mismo tiempo, el asesinato de tres agentes de policía y otro miembro del personal de la Jefatura de policía de París, el 3 de octubre de 2019, demuestra que la amenaza del terrorismo yihadista sigue siendo real y que deben continuar los esfuerzos en curso para ayudar a los Estados miembros a hacerle frente. La huida de miembros del EI/Daesh encarcelados en el contexto de acontecimientos recientes en el norte de Siria podría tener un grave impacto en la seguridad en Europa. Es importante que los Estados miembros hagan pleno uso de los sistemas de información existentes para detectar e identificar a los combatientes terroristas extranjeros que crucen las fronteras. También se están haciendo progresos en el uso de información del campo de batalla para procesar a los combatientes terroristas extranjeros.

El presente informe rinde cuentas de los avances recientes en el trabajo hacia una Unión de la Seguridad genuina y efectiva, destacando los ámbitos en los que se requieren nuevas medidas. Ofrece información actualizada sobre la aplicación de las medidas acordadas en materia de **ciberseguridad de las redes 5G**, en particular sobre el **Informe de evaluación de riesgos de la UE** publicado el 9 de octubre de 2019 y sobre la **lucha contra la desinformación**.

El presente informe se centra, en particular, en la **dimensión externa** de la cooperación en la Unión de la Seguridad, con la firma de dos acuerdos bilaterales de **lucha antiterrorista** con Albania y la República de Macedonia del Norte y los progresos realizados en la cooperación con terceros países socios en el intercambio de **datos relativos al registro de nombres de los pasajeros**. Además, junto con el presente informe, la Comisión adoptó una solicitud de autorización para el inicio de las negociaciones de un acuerdo entre la UE y **Nueva Zelanda** sobre el intercambio de datos personales para luchar contra la delincuencia grave y el terrorismo.

II. CUMPLIMIENTO DE LAS PRIORIDADES LEGISLATIVAS

1. *Prevenir la radicalización en línea y en las comunidades*

La **prevención de la radicalización** es la piedra angular de la respuesta de la Unión a las amenazas que plantea el terrorismo. A este respecto, Internet ha sido el campo de batalla más significativo de la acción terrorista en el siglo 21. Los espacios en los que las personas radicalizadas pueden comunicarse y compartir contenidos permiten el desarrollo de redes mundiales, ampliando las redes de yihadistas y de extremistas violentos de derechas. Esta es la razón por la que la Comisión continúa con su doble enfoque de la lucha contra la

radicalización en línea, en el que las normas propuestas para eliminar los contenidos terroristas ilícitos en línea deben reforzar la asociación voluntaria a plataformas en línea.

Resulta esencial para ello la **propuesta legislativa para prevenir la difusión de contenidos terroristas en línea**, con normas y salvaguardias claras que obliguen a las plataformas de Internet a retirar los contenidos terroristas en el plazo de una hora desde la recepción de una solicitud motivada de las autoridades competentes y adoptar medidas proactivas proporcionadas al nivel de exposición a contenidos terroristas[4]. Se están llevando a cabo negociaciones interinstitucionales entre el Parlamento Europeo y el Consejo, y se ha celebrado una primera reunión tripartita el 17 de octubre de 2019. Habida cuenta de la amenaza que representa el contenido terrorista en línea, la Comisión insta a los colegisladores a alcanzar un acuerdo sobre la legislación propuesta a finales de 2019.

La legislación propuesta complementa la asociación voluntaria con la industria de Internet y otras partes interesadas que tiene lugar en el **Foro de la UE sobre Internet**. Desde su creación en 2015, ha sido un catalizador para que las empresas de Internet actúen proactivamente para detectar y retirar contenidos terroristas en línea, allanando el camino para la iniciativa del sector de una «base de datos de hash compartida»[5] y la creación del Foro Mundial de Internet de lucha contra el terrorismo. La Unidad de Notificación de Contenidos de Internet de la UE, que forma parte de la agencia de seguridad de la UE, Europol, ha desempeñado un papel decisivo a la hora de reforzar la cooperación con las empresas de Internet y contribuir a la consecución de los objetivos generales del Foro de Internet de la UE. En la última reunión ministerial del Foro de Internet de la UE, celebrada el 7 de octubre de 2019, los Estados miembros de la UE y altos representantes de las empresas de Internet se comprometieron a colaborar en el marco del denominado **Protocolo de crisis de la UE**, que determina umbrales para la cooperación reforzada y establece nuevas formas de mejorar la respuesta a las crisis. Estas medidas forman parte de los esfuerzos realizados a nivel internacional para aplicar el «Llamamiento de Christchurch»[6], con el objetivo de garantizar una reacción coordinada y rápida a fin de contener la propagación de los contenidos terroristas o extremistas violentos en línea.

Más allá de estas medidas contra la radicalización en línea, la Comisión sigue apoyando los esfuerzos a nivel nacional y local para **prevenir y combatir la radicalización sobre el terreno**. Basándose en la riqueza de la experiencia y los conocimientos adquiridos en el marco de la Red para la Sensibilización frente a la Radicalización, la UE presta un apoyo específico a los agentes locales, incluidas las ciudades[7], y ofrece oportunidades de intercambio entre profesionales, investigadores y responsables políticos. La red, por ejemplo, ha formulado orientaciones específicas y ha organizado talleres en apoyo de las autoridades

---

4 COM (2018) 640 final de 12.9.2018.

5 Una herramienta creada por un consorcio de empresas para facilitar la cooperación a fin de evitar la difusión de contenidos terroristas en todas las plataformas.

6 En respuesta a los ataques perpetrados en Christchurch, Nueva Zelanda, el 15 de marzo de 2019, el presidente francés, Emmanuel Macron, y la primera ministra de Nueva Zelanda, Jacinda Ardern, invitaron a los dirigentes y plataformas en línea a París, el 15 de mayo de 2019, para poner en marcha el «Llamamiento de Christchurch». El presidente Juncker apoyó la convocatoria y anunció el desarrollo de un protocolo de crisis de la UE.

7 Sobre la cooperación con las ciudades en materia de seguridad, véase también la sección V.2 sobre la preparación y la protección, en particular la protección de los espacios públicos.

competentes que se hacen cargo de los menores procedentes de zonas de conflicto[8]. Para garantizar la continuidad de las actividades realizadas en el marco de la Red para la Sensibilización frente a la Radicalización, la Comisión ha iniciado el procedimiento de un nuevo contrato marco por un importe estimado de 61 millones EUR durante un período de cuatro años a partir de 2020[9].

Para hacer frente a la amenaza que representan los contenidos terroristas en línea, la Comisión insta al Parlamento Europeo y al Consejo a que:

- concluyan las negociaciones sobre la propuesta legislativa para evitar la difusión de **contenidos terroristas en línea** antes de finales de año.

2 *Sistemas de información más sólidos e inteligentes para la gestión de la seguridad, las fronteras y los flujos migratorios*

La UE ha intensificado el intercambio de información, facilitando la lucha contra la usurpación de identidad[10], reforzando los controles fronterizos[11], modernizando las bases de datos policiales en toda Europa[12], colmando las lagunas de información[13] y reforzando la agencia de seguridad de la UE, Europol[14]. Para ello es fundamental la **interoperabilidad de los sistemas de información de la UE**[15], lo que significa hacer el mejor uso posible de la información existente y eliminar los ángulos muertos. Respondiendo a las necesidades de

8 https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/radicalisation_awareness_network/ran-papers/docs/issue_paper_child_returnees_from_conflict_zones_112016_en.pdf

9 El contrato marco se divide en dos lotes: 29 000 000 EUR para apoyar las actividades de la Red de la UE para la Sensibilización frente a la Radicalización durante los próximos cuatro años y 32 000 000 EUR para reforzar las capacidades de los Estados miembros, las autoridades nacionales, regionales y locales y los terceros países prioritarios para luchar eficazmente contra la radicalización, en particular ofreciendo oportunidades de creación de redes, servicios orientados y centrados en las necesidades e investigación y análisis.

10 Reglamento (UE) 2019/1157, de 20.6.2019, 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.

11 Introducción de controles sistemáticos en las fronteras exteriores de todos los ciudadanos que utilicen el Sistema de Información de Schengen.

12 El Sistema de Información de Schengen reforzado [Reglamento (UE) 2018/1860 de 28.11.2018], Reglamento (UE) 2018/1861 de 28.11.2018 y el Reglamento (UE) 2018/1862 de 28.11.2018) y el Sistema Europeo de Información de Antecedentes Penales, ampliado a los nacionales de terceros países (Reglamento (UE) 2019/816 de 17.4.2019). El refuerzo del Sistema de Información de Schengen incluye la obligación general de introducir en el sistema descripciones relacionadas con el terrorismo.

13 El Sistema de Entradas y Salidas de la UE (Reglamento (UE) 2017/2226 de30.11.2017) y el Sistema Europeo de Información y Autorización de Viajes (Reglamento (UE) 2018/1240 de 12.9.2018 y Reglamento (UE) 2018/1241 de 12.9.2018).

14 En estos últimos años, se ha reforzado considerablemente el papel de Europol, tanto en extensión como en profundidad. La Agencia se ha reforzado con la adopción del Reglamento de Europol en 2016 (Reglamento (UE) 2016/794 de 11.5.2016). Los Estados miembros han aumentado considerablemente la cantidad de información compartida con Europol y a través de Europol. La creación del Centro Europeo de Lucha contra el Terrorismo (CELT) ha reforzado las capacidades analíticas de Europol en los casos de terrorismo. El presupuesto de Europol se ha incrementado constantemente en los últimos años, pasando de 82 millones EUR en 2014 a 138 millones EUR en 2019. Las negociaciones sobre el presupuesto para 2020 están en curso.

15 Reglamento (UE) 2019/817 de 20.5.2019 y Reglamento (UE) 2019/818 de 20.5.2019.

quienes trabajan en primera línea, la interoperabilidad permitirá un acceso más rápido y sistemático a la información de los agentes de los cuerpos de seguridad, los guardias de fronteras y los agentes de inmigración, contribuyendo así a mejorar la seguridad interior y la gestión de las fronteras.

Sin embargo, la interoperabilidad y toda la innovación que conlleva solo marcarán la diferencia en cuanto a la gestión de la seguridad, las fronteras y la migración sobre el terreno si cada Estado miembro aplica plenamente la legislación correspondiente. Esta es la razón por la que la **aplicación** de la interoperabilidad es una prioridad máxima de la Unión de la Seguridad, tanto a nivel político como técnico. La Comisión y la Agencia de la UE para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud en el Espacio de Libertad, Seguridad y Justicia (eu-LISA) apoyan a los Estados miembros aportando conocimientos especializados y mediante el intercambio de buenas prácticas, utilizando una red de coordinadores nacionales y desarrollando un cuadro de indicadores que permita una supervisión y coordinación eficaces. La estrecha cooperación entre las agencias de la UE, todos los Estados miembros y los países asociados a Schengen será fundamental para alcanzar el ambicioso objetivo de lograr la plena interoperabilidad de los sistemas de información de la UE para la gestión de la seguridad, las fronteras y la migración de aquí a 2020.

Mientras tanto, el Parlamento Europeo y el Consejo aún deben **completar el trabajo legislativo** a este respecto. Es fundamental un acuerdo rápido sobre todas las propuestas legislativas pendientes para garantizar el despliegue pleno y oportuno de la interoperabilidad. En primer lugar, como parte de la aplicación técnica del **Sistema Europeo de Autorización e Información sobre Viajes**, es necesario introducir modificaciones técnicas en los reglamentos[16] correspondientes para la plena implantación del sistema. La Comisión invita al Parlamento Europeo a que acelere sus trabajos sobre estas enmiendas técnicas con el fin de iniciar las negociaciones interinstitucionales lo antes posible. En segundo lugar, siguen en curso las negociaciones interinstitucionales sobre la propuesta de mayo de 2018 para reforzar y actualizar el actual **Sistema de Información de Visados**[17]. Tomando como la base de la primera reunión del diálogo tripartito, celebrada el 22 de octubre de 2019, la Comisión insta a ambos colegisladores a que concluyan rápidamente las negociaciones. En tercer lugar, sigue pendiente el acuerdo sobre la propuesta de la Comisión, de mayo de 2016, de ampliar el ámbito de aplicación de **Eurodac**[18] almacenando no solo las impresiones dactilares y los datos pertinentes de los solicitantes de asilo y de las personas interceptadas con ocasión de los cruces irregulares de las fronteras exteriores, sino también de los nacionales de terceros países en situación irregular. Los cambios propuestos también ampliarán el plazo de conservación de las impresiones dactilares y los datos pertinentes de quienes entran en la UE de forma irregular. La Comisión pide a los colegisladores que procedan a la adopción de la propuesta.

Con el fin 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 que:

- avancen en sus trabajos para alcanzar rápidamente un acuerdo sobre las modificaciones técnicas propuestas necesarias para establecer el **Sistema Europeo de Información y Autorización de Viajes**;

16 Reglamento (UE) 2018/1240 de 12.9.2018 y Reglamento (UE) 2018/1241 de 12.9.2018.
17 COM (2018) 302 final de 16.5.2018.
18 COM (2016) 272 final de 4.5.2016.

- lleven a cabo y concluyan rápidamente las negociaciones sobre la propuesta para reforzar el actual **Sistema de Información de Visados**;
- adopten la propuesta legislativa sobre **Eurodac** *(prioridad de una Declaración conjunta)*.

3. Restringir el perímetro de actuación de los terroristas

La UE ha adoptado medidas firmes para restringir el perímetro de actuación de los terroristas, con nuevas normas que dificultan que los terroristas y otros delincuentes accedan a explosivos[19], armas de fuego y financiación[20], así como para restringir su circulación[21].

Para reforzar la respuesta judicial al terrorismo, la Agencia Europea de Cooperación en materia de Justicia Penal (Eurojust) creó el 1 de septiembre de 2019 un **Registro Europeo de Lucha contra el Terrorismo**. Este registro reunirá información judicial para establecer vínculos en los procedimientos contra sospechosos de delitos de terrorismo, reforzando así la coordinación entre los fiscales en las investigaciones de lucha contra el terrorismo con posibles implicaciones transfronterizas.

No obstante, son necesarios esfuerzos adicionales para apoyar y facilitar las investigaciones en los asuntos transfronterizos, especialmente en lo que se refiere al **acceso a las pruebas electrónicas** por parte de los cuerpos de seguridad. Por lo que se refiere a las propuestas legislativas de abril de 2018 para mejorar el acceso transfronterizo a las pruebas electrónicas en las investigaciones penales[22], el Parlamento Europeo aún tiene que adoptar su posición antes de que los colegisladores puedan entablar negociaciones. La Comisión insta al Parlamento Europeo a que avance en esta propuesta legislativa para que los colegisladores puedan trabajar en pos de su rápida adopción. Sobre la base de su propuesta de normas internas de la UE, la Comisión también está llevando a cabo **negociaciones internacionales** para mejorar el acceso transfronterizo a las pruebas electrónicas. El 25 de septiembre de 2019, la Comisión y las autoridades estadounidenses celebraron la primera ronda formal de negociaciones sobre un **Acuerdo UE-EE.UU. sobre el acceso transfronterizo a las pruebas electrónicas**. Está prevista una nueva ronda para el 6 de noviembre de 2019. En el contexto de las negociaciones en curso del **Segundo Protocolo adicional al Convenio de Budapest sobre Ciberdelincuencia**, la Comisión participó en nombre de la Unión en tres sesiones de negociación, en julio, septiembre y octubre de 2019. Aunque se han hecho grandes progresos en estas negociaciones, aún deben tratarse temas importantes de gran interés para la Unión, como las garantías en materia de protección de datos. La negociación de un segundo Protocolo adicional continuará en noviembre de 2019 y a lo largo de 2020. Es importante progresar rápidamente en ambas negociaciones con el fin de promover la cooperación internacional en materia de intercambio de pruebas electrónicas, garantizando al mismo tiempo su compatibilidad con el Derecho de la Unión y las obligaciones que este impone a los Estados miembros, teniendo también en cuenta la evolución futura del Derecho de la Unión.

---

19 Reglamento (UE) 2019/1148, de 20.6.2019, sobre la comercialización y la utilización de precursores de explosivos. El Reglamento entró en vigor el 31 de julio de 2019 y será aplicable 18 meses después de su entrada en vigor.

20 Directiva (UE) 2019/1153, de 11.7.2019, por la que se establecen normas destinadas a facilitar el uso de información financiera y de otros tipos para la prevención, detección, investigación o enjuiciamiento de infracciones penales.

21 Introducción de controles sistemáticos en las fronteras exteriores de todos los ciudadanos que utilicen el Sistema de Información de Schengen.

22 COM (2018) 225 final de 17.4.2018 y COM (2018) 226 final de 17.4.2018.

Como expresión de la preocupación reinante por el blanqueo de capitales, el Parlamento Europeo adoptó el 19 de septiembre de 2019 una **Resolución sobre el estado de la aplicación de la legislación de la Unión contra el blanqueo de capitales**[23], en respuesta al paquete de cuatro informes sobre la lucha contra el blanqueo de capitales que la Comisión adoptó el 24 de julio de 2019[24]. El Parlamento Europeo insta a los Estados miembros a que garanticen la correcta y rápida aplicación de las directivas contra el blanqueo de capitales. El Parlamento Europeo también pide a la Comisión que evalúe la conveniencia de un reglamento contra el blanqueo de capitales en lugar de una directiva y la necesidad de un mecanismo de coordinación y apoyo a las unidades de inteligencia financiera.

Con el fin de mejorar el acceso de los cuerpos de seguridad a las pruebas electrónicas, la Comisión insta al Parlamento Europeo y al Consejo a que:

- alcancen rápidamente un acuerdo sobre las propuestas legislativas relativas a las **pruebas electrónicas** *(prioridad de una Declaración conjunta)*.

4. Reforzar la ciberseguridad

El refuerzo de la ciberseguridad continúa siendo un elemento clave del trabajo por una Unión de la Seguridad genuina y efectiva. Merced a la aplicación de la Estrategia de ciberseguridad de la UE de 2017[25], la Unión ha fortalecido su resiliencia, haciendo más difícil el ataque y más rápida la recuperación, así como su efecto disuasorio, aumentando las posibilidades de que los agresores sean capturados y castigados, también a través de un marco para una respuesta diplomática conjunta de la UE a las actividades cibernéticas malintencionadas. La Unión también apoya a los Estados miembros en el ámbito de la ciberdefensa, aplicando el marco político de ciberdefensa de la UE[26].

Con la entrada en vigor del Reglamento sobre la Ciberseguridad[27] en junio de 2019, está tomando forma el **marco de certificación de la ciberseguridad de la UE**. La certificación desempeña un papel fundamental para incrementar la confianza y la seguridad en productos y servicios que son cruciales para el mercado único digital. El marco de certificación proporcionará sistemas de certificación a escala de la UE, como un conjunto íntegro de normas, requisitos técnicos, estándares y procedimientos. Participan en esta labor dos grupos de expertos, a saber: el Grupo Europeo de Certificación de la Ciberseguridad, que representa a las autoridades de los Estados miembros, y el Grupo de Partes Interesadas en la Certificación de la Ciberseguridad, que representa a la industria. Este último reúne tanto al sector de la demanda como al de la oferta de productos y servicios de tecnologías de la información y la comunicación, incluidas las pequeñas y medianas empresas, los proveedores de servicios digitales, los organismos de normalización europeos e internacionales, los organismos

23 http://www.europarl.europa.eu/doceo/document/TA-9-2019-0022_ES.html

24 «Informe sobre la evaluación de los riesgos de blanqueo de capitales y financiación del terrorismo que afectan al mercado interior y están relacionados con actividades transfronterizas» [COM (2019) 370 (24.7.2019)], «Informe sobre la interconexión de los mecanismos centralizados automatizados nacionales (registros centrales o sistemas centrales electrónicos de consulta de datos) de los Estados miembros relacionados con las cuentas bancarias» [COM (2019) 372 final (24.7.2019)], «Informe sobre la evaluación de los recientes supuestos casos blanqueo de capitales con la implicación de entidades de crédito de la UE» [COM (2019) 373 final (24.7.2019)] e «Informe en el que se evalúa el marco de cooperación entre las unidades de inteligencia financiera» [COM (2019) 371 final de 24.7.2019]).

25 JOIN (2017) 450 final de 13.9.2017.

26 Marco político de ciberdefensa de la UE (actualización de 2018), adoptado por el Consejo el 19 de noviembre de 2018 (14413/18).

27 Reglamento (UE) 2019/881 de 17.4.2019.

nacionales de acreditación, las autoridades de supervisión de la protección de datos y los organismos de evaluación de la conformidad.

Mientras tanto, el Parlamento Europeo y el Consejo aún tienen que llegar a un acuerdo sobre la iniciativa legislativa[28] de un **Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y** una **Red de Centros Nacionales de Coordinación**. La propuesta tiene por objeto reforzar la capacidad de ciberseguridad de la Unión, estimulando el ecosistema europeo de ciberseguridad tecnológica e industrial, así como coordinar y poner en común los recursos conexos. La Comisión insta a ambos colegisladores a que reanuden y concluyan rápidamente las negociaciones interinstitucionales sobre esta iniciativa prioritaria para reforzar la ciberseguridad.

La labor de refuerzo de la ciberseguridad incluye un apoyo tanto nacional como regional[29].

Más allá de las amenazas cibernéticas contra sistemas y datos, la UE sigue enfrentándose a los complejos y polifacéticos desafíos planteados por las **amenazas híbridas**. En el Consejo, se ha creado un grupo de trabajo horizontal sobre la lucha contra las amenazas híbridas para mejorar la resiliencia de la UE y sus Estados miembros contra las amenazas híbridas y apoyar las medidas destinadas a reforzar la resistencia de las sociedades a las crisis. La Comisión y el Servicio Europeo de Acción Exterior apoyan estos esfuerzos con arreglo al marco conjunto para la lucha contra las amenazas híbridas de 2016[30] y la Comunicación conjuntan «Aumentar la resiliencia y desarrollar las capacidades para hacer frente a las amenazas híbridas» de 2018[31]. Además, el Centro Común de Investigación está elaborando un «modelo conceptual» para definir las amenazas híbridas, con el objetivo de ayudar a los Estados miembros y a sus autoridades competentes a identificar el tipo de ataque híbrido al que pueden enfrentarse. El modelo analiza cómo un agente (estatal o no) emplea una serie de herramientas (desde la desinformación al espionaje o las operaciones físicas) en diversos ámbitos (económico, militar, social, político) para alcanzar un blanco con miras a lograr una serie de objetivos.

Con el fin de mejorar la ciberseguridad, la Comisión insta al Parlamento Europeo y al Consejo a 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**.

III. MEJORAR LA SEGURIDAD DE LAS INFRAESTRUCTURAS DIGITALES

Las redes de quinta generación (5G) serán la futura espina dorsal de unas sociedades y economías cada vez más digitalizadas. Miles de millones de objetos y sistemas conectados se ven afectados, en particular en sectores críticos como la energía, el transporte, la banca y la sanidad, así como los sistemas de control industrial que transmiten información sensible y apoyan los sistemas de seguridad. Es fundamental, por lo tanto, garantizar la ciberseguridad y la resiliencia de las redes 5G.

---

28 COM (2018) 630 final de 12.9.2018.

29 Por ejemplo, la Comisión apoya una asociación interregional para la innovación en materia de ciberseguridad con la participación de Bretaña, Castilla y León, Renania del Norte-Westfalia, Finlandia central y Estonia para desarrollar una cadena de valor europea en materia de ciberseguridad, centrada en la comercialización y expansión.

30 JOIN (2016) 18 final de 6.4.2016.

31 JOIN (2018) 16 final de 13.6.2018.

Como parte de un enfoque coordinado, los Estados miembros publicaron el 9 de octubre de 2019 un informe sobre la **evaluación coordinada de los riesgos de la UE en materia de ciberseguridad en las redes 5G** con el apoyo de la Comisión y de la Agencia Europea para la Ciberseguridad[32]. Este importante paso forma parte del cumplimiento de la Recomendación de la Comisión de marzo de 2019 para garantizar un alto nivel de ciberseguridad de las redes 5G en toda la UE[33]. El informe se basa en los resultados de las evaluaciones nacionales de los riesgos en materia de ciberseguridad de todos los Estados miembros. Identifica los principales riesgos y amenazas, los activos más sensibles, las principales vulnerabilidades (incluidas las vulnerabilidades técnicas y de otros tipos) y una serie de riesgos estratégicos. Esta evaluación sirve de base para determinar las medidas de mitigación que pueden aplicarse a nivel nacional y europeo.

El informe señala una serie de importantes **desafíos en materia de ciberseguridad** que pueden aparecer o adquirir más relevancia en las redes 5G. Estos retos en materia de seguridad están relacionados principalmente con las *innovaciones* clave de la tecnología 5G, en particular la importancia de los programas informáticos y la amplia gama de servicios y aplicaciones que permite la 5G, así como la función de los *proveedores* en la construcción y explotación de las redes 5G y el grado de dependencia de los proveedores. Esto significa que los productos, servicios y operaciones de los proveedores forman cada vez más parte de la «superficie de ataque» de las redes 5G. Además, el perfil de riesgo de los proveedores será especialmente importante, incluida la probabilidad de que el proveedor esté sujeto a la interferencia de un país no perteneciente a la UE.

De conformidad con el proceso establecido en la Recomendación de la Comisión de marzo de 2019, los Estados miembros deben acordar, a más tardar el 31 de diciembre de 2019, una **serie de medidas de mitigación** para hacer frente a los riesgos de ciberseguridad detectados a nivel nacional y de la Unión. La Comisión y el Servicio Europeo de Acción Exterior proseguirán también sus intercambios sobre la ciberseguridad y la resiliencia de las redes 5G con socios afines. En este sentido, la Comisión está en contacto con la OTAN a propósito de la evaluación coordinada de los riesgos de la ciberseguridad de las redes 5G.

IV. CONTRARRESTAR LA DESINFORMACIÓN Y PROTEGER LAS ELECCIONES FRENTE A OTRAS AMENAZAS CIBERNÉTICAS

La UE ha establecido un **marco para la acción coordinada contra la desinformación**, que respeta plenamente los valores europeos y los derechos fundamentales[34]. En el marco del Plan de Acción contra la Desinformación[35], se continúa trabajando para no dejar espacio a la desinformación, también con el fin de proteger la integridad de las elecciones.

Resulta esencial para ello el trabajo con la industria mediante el **Código de buenas prácticas sobre desinformación** para las plataformas en línea y el sector publicitario, que entró en

---

32 La evaluación coordinada de los riesgos en materia de ciberseguridad en las redes 5G realizada por la UE fue completada por el Grupo de cooperación de las autoridades competentes según lo establecido en la Directiva sobre seguridad de las redes y sistemas de información (Directiva (UE) 2016/1148, de 6.7.2016), con la ayuda de la Comisión y de la Agencia Europea para la Ciberseguridad: https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security.

33 C (2019) 2355 final de 26.3.2019.

34 Véase el Plan de acción contra la desinformación [JOIN (2018) 36 final de 5.12.2018].

35 JOIN (2019) 12 final de 14.6.2019.

vigor en octubre de 2018[36]. La Comisión ha evaluado la eficacia del Código tras su primer año de funcionamiento, sobre la base de los informes de autoevaluación anuales presentados por las plataformas en línea y por los demás signatarios del Código, publicados el 29 de octubre de 2019 junto con una Declaración de la Comisión[37]. En términos generales, los informes muestran el gran esfuerzo de los firmantes para cumplir sus compromisos.

Las acciones llevadas a cabo por las plataformas signatarias varían en cuanto a su rapidez y alcance entre los cinco pilares de compromisos del Código. En general, se han hecho más progresos en los compromisos relativos a las elecciones europeas de 2019, a saber, sobre publicidad perturbadora e incentivos a la monetización de la desinformación (pilar 1), garantizar la transparencia de la publicidad política y temática (pilar 2) y garantizar la integridad de los servicios frente a las cuentas y los comportamientos inauténticos (pilar 3). Por el contrario, ha habido menos avances o se han hecho progresos insuficientes con respecto a los compromisos de capacitar a los consumidores (pilar 4) y capacitar a la comunidad de investigación, también mediante la oferta, a través de plataformas, de un acceso pertinente y respetuoso con la privacidad a conjuntos de datos con fines de investigación (pilar 5). Se observan asimismo diferencias en el alcance de las acciones emprendidas por cada plataforma para garantizar el cumplimiento de sus compromisos, así como entre los Estados miembros en la aplicación de las distintas políticas. La Comisión sigue trabajando con los firmantes del Código y con otras partes interesadas para intensificar las medidas adoptadas contra la desinformación.

En el marco del Plan de Acción contra la Desinformación, la Comisión y la Alta Representante, en cooperación con los Estados miembros, crearon un **sistema de alerta rápida** para hacer frente a las campañas de desinformación. El sistema de alerta rápida permitió a las instituciones de la UE y a los Estados miembros compartir información y análisis antes de las elecciones de 2019 al Parlamento Europeo y coordinar las respuestas. Este trabajo se ha intensificado tras las elecciones, con intercambios diarios de información operativa y tres reuniones de los puntos de contacto de los sistemas de alerta rápida organizadas por distintos Estados miembros.

Otro adelanto práctico para detectar la desinformación ha sido el trabajo del **Equipo de Comunicación Estratégica** («Stratsms»), y en particular su Grupo de Trabajo «East Stratcom», que gestiona el proyecto «EUvsDisinfo» para supervisar, analizar y responder a la desinformación favorable al Kremlin[38]. Desde principios de 2019, el primer presupuesto específico de 3 millones EUR ha permitido aumentar y ampliar este trabajo a fin de incluir el seguimiento y el análisis de la desinformación favorable al Kremlin en la web, la radiodifusión y los medios sociales en 19 lenguas, desde el inglés hasta el serbio y el árabe. La cantidad de actividades de desinformación expuestas se duplicó con creces debido a la

---

36 En virtud del Código, las plataformas en línea Google, Facebook, Twitter y Microsoft se han comprometido a prevenir el uso manipulador de sus servicios por parte de agentes maliciosos, ofrecer transparencia y divulgación pública de la publicidad política, y adoptar otras medidas para mejorar la transparencia, la rendición de cuentas y la fiabilidad del ecosistema en línea. Las organizaciones profesionales del sector de la publicidad también se han comprometido a cooperar con las plataformas para mejorar el control de los espacios publicitarios y desarrollar herramientas de seguridad de marca destinadas a limitar la colocación de publicidad en sitios web que divulgue desinformación.

37 https://ec.europa.eu/commission/presscorner/detail/en/statement_19_6166. Además de Google, Facebook, Twitter y Microsoft, entre los demás signatarios del Código figuran Mozilla, siete asociaciones europeas o nacionales que representan al sector de la publicidad y EDiMA, una asociación europea que representa a plataformas y otras empresas tecnológicas activas en el sector en línea.

38 www.euvsdisinfo.eu.

mejora de la capacidad de control, con cerca de 2 000 casos de desinformación hasta la fecha en 2019, frente a 765 casos en ese mismo período de 2018. El Grupo de Trabajo «East Stratcom» desempeñó un papel fundamental en el seguimiento y exposición de desinformación a favor del Kremlin contra las elecciones de 2019 al Parlamento Europeo. La investigación se acompañó de una campaña de sensibilización sobre los intentos de interferencia en los procesos electorales en todo el mundo. Su alcance, en estrecha cooperación con el Parlamento Europeo y la Comisión, se tradujo en más de 20 entrevistas con medios de comunicación, y en la campaña participaron más de 300 periodistas.

La Comisión también ha tomado medidas para **reducir la difusión de desinformación y mitos sobre las instituciones y las políticas de la UE**. Ha creado una red de expertos en comunicación con un portal en línea que ofrece material informativo interactivo sobre las políticas de la UE y el reto de la desinformación y su impacto en la sociedad. También ha puesto en marcha una serie de campañas en las redes sociales centradas en la lucha contra la desinformación[39], en colaboración con el Parlamento Europeo y el Servicio Europeo de Acción Exterior.

V. EJECUCIÓN DE OTRAS MEDIDAS PRIORITARIAS EN MATERIA DE SEGURIDAD

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

Las medidas acordadas en la Unión de la Seguridad solo aportarán plenos beneficios a la seguridad si todos los Estados miembros garantizan su rápida e íntegra aplicación. Con este fin, la Comisión apoya activamente a los Estados miembros en la aplicación de la legislación de la UE, en particular mediante financiación y facilitando el intercambio de buenas prácticas. La Comisión hace pleno uso de sus competencias en virtud de los Tratados para la aplicación de la legislación de la UE, incluido, en su caso, el procedimiento de infracción.

El plazo para la transposición de la **Directiva sobre el registro de nombres de los pasajeros de la UE**[40] expiró el 25 de mayo de 2018. Hasta la fecha, 25 Estados miembros han notificado su plena transposición[41], lo que representa un avance significativo desde julio de 2018, cuando la Comisión inició procedimientos de infracción contra 14 Estados miembros[42]. Dos Estados miembros no han notificado aún la plena transposición, a pesar de los procedimientos de infracción en curso iniciados el 19 de julio de 2018[43]. 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 buenas prácticas.

---

39 https://europa.eu/euprotects/.

40 Directiva (UE) 2016/681 de 27.4.2016. Dinamarca no participó en la adopción de esta Directiva y no está vinculada por ella ni sujeta a su aplicación.

41 Las referencias a la notificación de la plena transposición tienen en cuenta las declaraciones de los Estados miembros y se entienden sin perjuicio de la comprobación de la transposición por parte de los servicios de la Comisión (situación a 17.10.2019).

42 Véase el Decimosexto informe sobre la evolución hacia una Unión de la Seguridad genuina y efectiva [COM (2018) 690 final de 10.10.2018].

43 Eslovenia ha notificado su transposición parcial. España no ha notificado la transposición (situación a 17.10.2019).

El plazo para la transposición de la **Directiva relativa a la lucha contra el terrorismo**[44] expiró el 8 de septiembre de 2018. Hasta la fecha, 22 Estados miembros han notificado la plena transposición, lo que representa un avance significativo desde noviembre de 2018, cuando la Comisión inició procedimientos de infracción contra 16 Estados miembros[45]. Tres Estados miembros no han notificado aún la plena transposición, a pesar de los procedimientos de infracción en curso[46]. El 25 de julio de 2019, la Comisión envió dictámenes motivados a dos Estados miembros por no haber notificado la plena transposición de la Directiva[47]. En su respuesta, ambos Estados miembros han anunciado que los trabajos legislativos concluirán antes de finales de este año.

El plazo para la transposición de la **Directiva sobre el control de la adquisición y tenencia de armas**[48] expiró el 14 de septiembre de 2018. Hasta la fecha, 13 Estados miembros han notificado la plena transposición. Pero 15 Estados miembros no han notificado aún la plena transposición, a pesar de los procedimientos de infracción en curso iniciados el 22 de noviembre de 2018[49]. El 25 de julio de 2019, la Comisión envió dictámenes motivados a 20 Estados miembros por no haber notificado la plena transposición de la Directiva. En su respuesta, cinco Estados miembros han notificado la plena transposición de la Directiva[50].

El plazo para la transposición de la **Directiva sobre protección de datos**[51] expiró el 6 de mayo de 2018. Hasta la fecha, 25 Estados miembros han notificado su plena transposición, lo que representa un avance significativo desde julio de 2018, cuando la Comisión inició procedimientos de infracción contra 19 Estados miembros[52]. Tres Estados miembros no han notificado aún su plena transposición, a pesar de los procedimientos de infracción en curso[53]. El 25 de julio de 2019, la Comisión decidió remitir a dos Estados miembros[54] al Tribunal de Justicia de la Unión Europea por falta de transposición de la Directiva y envió una carta de emplazamiento a un Estado miembro[55] por no transponer plenamente la Directiva[56].

La Comisión está evaluando la transposición de la **4.ª Directiva contra el blanqueo de capitales**[57], al tiempo que trabaja para verificar que los Estados miembros aplican sus normas.

---

44 Directiva (UE) 2017/541 de 15.3.2017. Esta Directiva no es aplicable en el Reino Unido, Irlanda y Dinamarca.

45 Véase el Decimoséptimo informe sobre la evolución hacia una Unión de la Seguridad genuina y efectiva [COM (2018) 845 final de 11.12.2018].

46 Grecia y Luxemburgo no han notificado las medidas nacionales de ejecución. Polonia ha notificado medidas nacionales de transposición parcial (situación a 17.10.2019).

47 Grecia y Luxemburgo.

48 Directiva (UE) 2017/853 de 17.10.2019.

49 Bélgica, Chequia, Estonia, Polonia, Suecia, Eslovaquia y Reino Unido han notificado medidas de transposición de una parte de las nuevas disposiciones. Chipre, Alemania, Grecia, España, Luxemburgo, Hungría, Rumanía y Eslovenia no han notificado ninguna medida de transposición (situación a 17.10.2019).

50 Finlandia, Irlanda, Lituania, Países Bajos y Portugal (situación a 17.10.2019).

51 Directiva (UE) 2016/680 de 27.4.2016.

52 Véase el Decimosexto informe sobre la evolución hacia una Unión de la Seguridad genuina y efectiva [COM (2018) 690 final de 10.10.2018].

53 Eslovenia notificó su transposición parcial. España no notificó su transposición. Aunque Alemania ha notificado su plena transposición, la Comisión considera que la transposición es incompleta (situación a partir de 17.10.2019).

54 Grecia y España.

55 Alemania.

56 Grecia notificó la plena transposición, que la Comisión está evaluando.

57 Directiva (UE) 2015/849 de 20.5.2015.

Debían transponer la Directiva a su legislación nacional el 26 de junio de 2018 a más tardar. La Comisión mantiene abiertos procedimientos de infracción contra 21 Estados miembros, ya que consideró que la notificación recibida de estos Estados miembros no constituye una plena transposición de la Directiva[58].

La Comisión ha evaluado la conformidad de la transposición de las **Directivas sobre ciberseguridad**. En julio y octubre de 2019, incoó procedimientos de infracción contra 23 Estados miembros[59] al entender que la legislación nacional de aplicación notificada por esos Estados miembros no constituye una correcta transposición de la **Directiva relativa a la lucha contra el abuso sexual de menores**[60]. La Comisión también inició en julio y octubre de 2019 procedimientos de infracción contra cuatro Estados miembros[61], al entender que la legislación nacional de aplicación notificada por esos Estados miembros no constituye una transposición correcta de la **Directiva relativa a los ataques contra los sistemas de información**[62].

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

- La **Directiva de la UE relativa al registro de nombres de los pasajeros**, sobre la que 1 Estado miembro aún debe notificar su transposición al Derecho nacional y 1 Estado miembro aún debe completar la notificación de su transposición[63].
- La **Directiva relativa a la lucha contra el terrorismo**, sobre la que 2 Estados miembros aún deben notificar su transposición al Derecho nacional y 1 Estado miembro aún debe completar la notificación de su transposición[64].
- La **Directiva sobre el control de la adquisición y tenencia de armas**, sobre la que 8 Estados miembros aún deben notificar su transposición al Derecho nacional y 7 Estados miembros aún deben completar la notificación de su transposición[65].
- La **Directiva sobre protección de datos,** sobre la que 1 Estado miembro aún debe notificar su transposición al Derecho nacional y 2 Estados miembros aún deben completar la notificación de su transposición[66].

---

58 Bélgica, Bulgaria, Chequia, Dinamarca, Alemania, Estonia, Irlanda, Francia, Italia, Chipre, Letonia, Lituania, Hungría, Países Bajos, Austria, Polonia, Rumanía, Eslovaquia, Finlandia, Suecia y el Reino Unido (situación a 17.10.2019). Anteriormente, se archivaron 7 procedimientos de infracción relacionados con la Directiva.

59 Bélgica, Bulgaria, Chequia, Alemania, Estonia, Grecia, España, Francia, Croacia, Italia, Letonia, Lituania, Luxemburgo, Hungría, Malta, Austria, Polonia, Portugal, Rumanía, Eslovenia, Eslovaquia, Finlandia y Suecia.

60 Directiva 2011/93/UE de 13.12.2011.

61 Bulgaria, Italia, Portugal y Eslovenia.

62 Directiva 2013/40/UE de 12.08.2013.

63 Eslovenia notificó su transposición parcial. España no ha notificado su transposición (situación a 17.10.2019).

64 Grecia y Luxemburgo no han notificado su transposición. Polonia ha notificado su transposición parcial (situación a 17.10.2019).

65 Bélgica, Chequia, Estonia, Polonia, Suecia, Eslovaquia y Reino Unido han notificado medidas de transposición de una parte de las nuevas disposiciones. Chipre, Alemania, Grecia, España, Luxemburgo, Hungría, Rumanía y Eslovenia no han notificado ninguna medida de transposición (situación a 17.10.2019).

66 Eslovenia ha notificado su transposición parcial. España no ha notificado su transposición. Aunque Alemania ha notificado su plena transposición, la Comisión considera que la transposición es incompleta (situación a 17.10.2019).

- La **4.ª Directiva contra el blanqueo de capitales**, sobre la que 21 Estados miembros aún no han completado la notificación de su transposición[67].
- La **Directiva relativa a la lucha contra el abuso sexual de menores,** sobre la que se han iniciado procedimientos de infracción por transposición incorrecta contra 23 Estados miembros[68].
- La **Directiva relativa a los ataques contra los sistemas de información**, sobre la que se han iniciado procedimientos de infracción por transposición incorrecta contra 4 Estados miembros[69].

2. Preparación y protección

Reforzar la resiliencia frente a las amenazas a la seguridad es una parte esencial de la labor encaminada a lograr una Unión de la Seguridad genuina y efectiva. La Comisión apoya a los Estados miembros y a las autoridades locales en la mejora de la protección de los espacios públicos, aplicando el Plan de Acción de octubre de 2017 y la Asociación para la Seguridad en los Espacios Públicos de enero de 2019 en el marco de la Agenda Urbana de la UE. Esta iniciativa incluye a las ciudades que se pusieron en contacto con la Comisión y pidieron apoyo para hacer frente a los retos a los que se enfrentan en la protección de los espacios públicos.

El intercambio de buenas prácticas entre las autoridades locales y con los operadores privados es fundamental para reforzar la seguridad de los espacios públicos. Este objetivo fue el centro de interés de la **Semana Europea de la Seguridad** celebrada en Niza, Francia, del 14 al 18 de octubre de 2019, y organizada por el proyecto financiado por la UE «Proteger las ciudades aliadas contra el terrorismo». El acto, que reunió a 500 participantes de ciudades de toda Europa, autoridades nacionales y centros de investigación, destacó la importancia de una estrecha cooperación entre todas las partes interesadas, tanto públicas como privadas, y el papel de las nuevas tecnologías en una mejor protección de las ciudades. La protección de los espacios públicos también figuró en el programa de la **Semana Europea de las Regiones y Ciudades** celebrada en Bruselas del 7 al 10 de octubre de 2019, con un taller sobre la Agenda Urbana de la Asociación de la UE para la Seguridad en los Espacios Públicos. Se centró en el papel de las autoridades locales en el ámbito de la política de seguridad, en la reglamentación y la financiación de la UE para hacer frente a los principales retos en materia de seguridad en los espacios públicos urbanos y en temas clave como la innovación mediante soluciones y tecnologías inteligentes, incluido el concepto de seguridad desde el diseño, la prevención y la inclusión social. La Comisión también está contribuyendo a fomentar la innovación de las ciudades en estos ámbitos a través de su última convocatoria de propuestas de Acciones Urbanas Innovadoras, cuyos resultados se anunciaron en agosto de 2019. Entre los proyectos seleccionados, tres ciudades (El Pireo en Grecia, Tampere en Finlandia y Turín en Italia) probarán nuevas soluciones en materia de seguridad urbana[70].

---

67 Bélgica, Bulgaria, Chequia, Dinamarca, Alemania, Estonia, Irlanda, Francia, Italia, Chipre, Letonia, Lituania, Hungría, Países Bajos, Austria, Polonia, Rumanía, Eslovaquia, Finlandia, Suecia y el Reino Unido (situación a 17.10.2019).

68 Bélgica, Bulgaria, Chequia, Alemania, Estonia, Grecia, España, Francia, Croacia, Italia, Letonia, Lituania, Luxemburgo, Hungría, Malta, Austria, Polonia, Portugal, Rumanía, Eslovenia, Eslovaquia, Finlandia y Suecia.

69 Bulgaria, Italia, Portugal y Eslovenia.

70 Las Acciones Urbanas Innovadoras son un instrumento cofinanciado por el desarrollo regional europeo. Para más información, véase: https://www.uia-initiative.eu/en/call-proposals/4th-call-proposals.

Para **proteger mejor los lugares de culto** y explorar las necesidades de los distintos grupos religiosos, la Comisión organizó el 7 de octubre de 2019 una reunión con representantes de las comunidades judía, musulmana, cristiana y budista. Parte integrante de la ejecución del «Plan de Acción de la UE para contribuir a la protección de los espacios públicos» de 2017, la reunión puso de manifiesto que la concienciación y la preparación en materia de seguridad varían significativamente entre las distintas comunidades religiosas, lo que subraya la importancia de un mayor intercambio de buenas prácticas. La reunión también puso de relieve que la adopción de medidas básicas de seguridad y una mayor sensibilización en materia de seguridad no son incompatibles con el mantenimiento del carácter abierto y accesible de los lugares de culto. La Comisión recopilará las buenas prácticas y los materiales de sensibilización en su plataforma electrónica para expertos y pondrá el asunto en conocimiento de las autoridades de seguridad de los Estados miembros en el foro público-privado para la protección de los espacios públicos.

Un ámbito específico que requiere mayor atención es el aumento de la amenaza para la seguridad de las infraestructuras y los espacios públicos críticos que representan los **drones**. La Comisión, como complemento de la legislación reciente de la UE[71] sobre las operaciones seguras de drones en el espacio aéreo de las aeronaves tripuladas, y sin menoscabo de las oportunidades para un uso beneficioso de los drones, apoya a los Estados miembros en su seguimiento de las tendencias del uso malintencionado de los drones, su financiación de la investigación pertinente y su respaldo al ensayo de contramedidas. Es fundamental el intercambio de experiencias y buenas prácticas, como demuestra la Conferencia internacional de alto nivel sobre la lucha contra las amenazas planteadas por los sistemas de aeronaves no tripuladas celebrada en Bruselas el 17 de octubre de 2019. Este acto, organizado por la Comisión, reunió a 250 participantes de los Estados miembros, organizaciones internacionales, socios de terceros países, la industria, el mundo académico y la sociedad civil para debatir sobre los retos que plantean los drones en materia de seguridad y la forma de hacerles frente. La reunión puso de manifiesto la necesidad de realizar periódicamente evaluaciones del riesgo que suponen los drones y de una estrecha cooperación entre las autoridades policiales y de aviación en el desarrollo de la legislación europea en materia de operaciones seguras de los drones. También es necesario seguir analizando las contramedidas en respuesta a los drones mediante un enfoque europeo coordinado. Además, se convino en que, para que los drones sean seguros, de confianza, operativamente fiables y difíciles de utilizar con fines malintencionados, resulta esencial un compromiso estrecho entre las autoridades y la industria.

3. Dimensión exterior

Dado que la mayoría de los riesgos de seguridad a los que se enfrenta la Unión trascienden las fronteras de la UE y representan amenazas globales, la cooperación con los países socios, las organizaciones y las partes interesadas pertinentes desempeña un papel fundamental en la creación de una Unión de la Seguridad genuina y efectiva.

El intercambio de información es fundamental para esta cooperación. Junto con el presente informe, la Comisión ha adoptado una recomendación al Consejo para que autorice la apertura de negociaciones de un **acuerdo entre la UE y Nueva Zelanda sobre el intercambio de datos personales para luchar contra la delincuencia grave y el**

[71] 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.

terrorismo entre Europol y las autoridades competentes de Nueva Zelanda. Dicho acuerdo reforzará la capacidad de Europol para colaborar con Nueva Zelanda con fines de prevención y lucha contra los delitos que forman parte del ámbito de competencias de Europol. Si bien el acuerdo de trabajo de abril de 2019 entre Europol y la policía de Nueva Zelanda proporciona un marco para la cooperación estructurada a nivel estratégico, no ofrece una base jurídica para el intercambio de datos personales. El intercambio de datos personales con pleno respeto del Derecho de la UE y de los derechos fundamentales resulta esencial para una cooperación policial operativa eficaz. Anteriormente, la Comisión identificó ocho países prioritarios en la región de Oriente Medio/Norte de África en función de la amenaza terrorista, los retos relacionados con la migración y las necesidades operativas de Europol para entablar las negociaciones[72]. Teniendo en cuenta las necesidades operativas de las autoridades policiales en la UE y los beneficios potenciales de una cooperación más estrecha en este ámbito, como así lo demuestra también el seguimiento del ataque de Navidad de marzo de 2019, la Comisión considera necesario añadir a Nueva Zelanda como país prioritario para iniciar las negociaciones a corto plazo.

Otra piedra angular de la cooperación de la Unión en materia de seguridad con terceros países es la transferencia de **datos del registro de nombres de los pasajeros**. El 27 de septiembre de 2019, la Comisión adoptó una Recomendación al Consejo para que autorice la apertura de negociaciones de un **acuerdo entre la UE y Japón** sobre la transferencia de datos del registro de nombres de pasajeros, con el fin de prevenir y combatir el terrorismo y los delitos transnacionales graves, respetando plenamente las salvaguardias y los derechos fundamentales en materia de protección de datos[73]. El grupo de trabajo del Consejo está examinando la recomendación y la Comisión insta al Consejo a que adopte rápidamente un mandato de negociación con Japón. Disponer de mecanismos a tiempo para los Juegos Olímpicos de 2020 aportaría un dividendo real en materia de seguridad.

A escala mundial, la Comisión apoya el trabajo realizado por la **Organización de Aviación Civil Internacional** a fin de establecer un estándar para el tratamiento de los datos del registro de nombres de los pasajeros. Responde al llamamiento de la Resolución 2396 del Consejo de Seguridad de las Naciones Unidas, que insta a todos los Estados miembros de las Naciones Unidas a que desarrollen la capacidad de recopilar, procesar y analizar los datos del registro de nombres de los pasajeros. El 13 de septiembre de 2019, la Comisión presentó una propuesta[74] de Decisión del Consejo relativa a la posición que debe adoptarse en nombre de la UE en la Organización de Aviación Civil Internacional respecto a las normas y prácticas recomendadas relativas a los datos del registro de nombres de los pasajeros. La propuesta está siendo examinada en el grupo de trabajo del Consejo y la Comisión insta a la rápida adopción de la Decisión del Consejo. La posición de la Unión y de sus Estados miembros también se expuso en el documento informativo «Normas y principios de la recopilación, el uso, el tratamiento y la protección de datos del registro de nombres de los pasajeros», que se presentó al 40.º período de sesiones de la Asamblea de la Organización de Aviación Civil Internacional.

Por lo que se refiere a los trabajos en pro de un nuevo acuerdo con **Canadá** sobre el registro de nombres de los pasajeros, la Comisión procura la rápida conclusión del acuerdo.

---

72 Véase el Undécimo informe sobre la evolución hacia una Unión de la Seguridad genuina y efectiva [COM (2017) 608 final de 18.10.2017]. Los países prioritarios son Argelia, Egipto, Israel, Jordania, Líbano, Marruecos, Túnez y Turquía.

73 COM (2019) 420 final de 27.9.2019.

74 COM (2019) 416 final de 13.9.2019.

Entretanto, la revisión y la evaluación conjunta del acuerdo con **Australia** sobre el registro de nombres de los pasajeros, así como la evaluación conjunta del acuerdo con **Estados Unidos** sobre el registro de nombres de los pasajeros, se pusieron en marcha este verano, empezando por las visitas a Canberra y a Washington en agosto y septiembre de 2019, respectivamente. La Comisión informó a la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo, en una sesión a puerta cerrada celebrada el 14 de octubre de 2019, sobre la situación de los trabajos con Japón, Australia y Canadá sobre el registro de nombres de los pasajeros.

También se ha avanzado en la cooperación en materia de seguridad con los socios de los **Balcanes Occidentales**, mediante la ejecución del Plan de acción conjunto en materia de lucha contra el terrorismo en los Balcanes Occidentales de octubre de 2018. El 9 de octubre, la Comisión firmó dos acuerdos bilaterales de lucha antiterrorista no vinculantes con Albania y la República de Macedonia del Norte[75]. Estos acuerdos establecen las medidas prioritarias específicas que deben adoptar las autoridades del país socio, que abarcan los cinco objetivos del Plan de acción conjunto[76] e indican el apoyo que la Comisión tiene intención de prestar. Se espera que en las próximas semanas se firmen acuerdos similares con los restantes socios de los Balcanes Occidentales. Además, el 7 de octubre de 2019, la Comisión firmó con Montenegro un acuerdo de cooperación en materia de gestión de fronteras entre Montenegro y la Agencia Europea de la Guardia de Fronteras y Costas (Frontex). Este acuerdo permite a la Agencia ayudar a Montenegro en la gestión de las fronteras con el objetivo de luchar contra la migración irregular y la delincuencia transfronteriza, reforzando así la seguridad en las fronteras exteriores de la UE.

Con el fin de reforzar la cooperación con los países socios para hacer frente a las amenazas comunes a la seguridad, la Comisión insta al Consejo a que:

- apruebe la apertura de negociaciones de un acuerdo entre la UE y **Nueva Zelanda** sobre el intercambio de datos personales para la lucha contra la delincuencia grave y el terrorismo;
- adopte la autorización para el inicio de negociaciones de un acuerdo entre la UE y **Japón** sobre la transferencia de datos relativos al registro de nombres de los pasajeros;
- adopte la propuesta de **Decisión del Consejo relativa a la posición que debe adoptarse en nombre de la UE en la Organización de Aviación Civil Internacional** en lo que respecta a las normas y métodos recomendados sobre los datos del registro de nombres de los pasajeros.

VI. CONCLUSIÓN

El presente informe expone la amplia gama de medidas que la UE ha adoptado para hacer frente a las amenazas comunes en Europa y reforzar nuestra seguridad colectiva. Guiado por el entendimiento común de que la mejor manera de hacer frente a los desafíos actuales a la seguridad es trabajar juntos y con terceros países, el progreso hacia una Unión de la Seguridad genuina y efectiva es el resultado de la estrecha cooperación entre un gran número de actores,

[75] https://ec.europa.eu/home-affairs/news/news/20191009_security-union-implementing-counter-terrorism-arrangements-albania-north-macedonia_en

[76] El Plan de acción conjunto prevé acciones con los cinco objetivos siguientes: un marco sólido para la lucha contra el terrorismo; la prevención eficaz y la lucha contra el extremismo violento; el intercambio efectivo de información y la cooperación operativa; la creación de capacidad para luchar contra el blanqueo de capitales y contra la financiación del terrorismo; el refuerzo de la protección de los ciudadanos y de las infraestructuras.

la creación de confianza, la puesta en común de recursos y la respuesta común a las amenazas: en todos los niveles de gobierno, desde las ciudades y otros entes locales, las regiones y las autoridades nacionales hasta el nivel de la UE, con el Parlamento Europeo y el Consejo; mediante la participación de las autoridades públicas, las agencias de la UE, el sector privado y la sociedad civil, y sirviéndose de los conocimientos, herramientas y recursos en todos los ámbitos políticos, como la política de transportes, el mercado único digital o la política de cohesión. De este modo, el trabajo en la Unión de la Seguridad se integra en la labor de protección de los derechos fundamentales, la salvaguarda y la promoción de nuestros valores.

El trabajo en pos de una Unión de la Seguridad genuina y efectiva debe proseguir. Es necesario un acuerdo rápido sobre importantes iniciativas pendientes, en particular: 1) la propuesta legislativa sobre la eliminación de contenidos terroristas en línea; 2) la propuesta legislativa para mejorar el acceso de los cuerpos de seguridad a las pruebas electrónicas; 3) la propuesta legislativa por la que se crea un Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación, y 4) las propuestas legislativas pendientes sobre unos sistemas de información más sólidos e inteligentes para la gestión de la seguridad, las fronteras y la migración. Las medidas e instrumentos acordados deben transformarse en una realidad operativa sobre el terreno, con la plena y oportuna aplicación de la legislación de la UE por parte de todos los Estados miembros para cosechar todos sus beneficios en materia de seguridad. En particular, es esencial que todos los Estados miembros apliquen la legislación recientemente acordada sobre la interoperabilidad de los sistemas de información de la UE para la gestión de la seguridad, las fronteras y la migración con el fin de alcanzar el ambicioso objetivo de lograr la plena interoperabilidad para 2020. Por último, Europa debe permanecer alerta ante las amenazas emergentes y cambiantes, y seguir trabajando en común para mejorar la seguridad de todos los ciudadanos.