COMISIÓN
EUROPEA

Bruselas, 20.3.2019
COM(2019) 145 final

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

Decimoctavo informe sobre la evolución hacia una Unión de la Seguridad genuina y efectiva

{SWD(2019) 140 final}

I. INTRODUCCIÓN

Este es el decimoctavo informe sobre los avances realizados en la configuración de una Unión de la Seguridad genuina y efectiva. Abarca la evolución en torno a dos grandes pilares: 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.

En la perspectiva de las elecciones al Parlamento Europeo de mayo de 2019, el presente informe subraya la importante labor realizada a distintos niveles para abordar y prevenir las amenazas cibernéticas y la desinformación en el contexto electoral. En respuesta al llamamiento del Consejo Europeo en favor de medidas que protejan los sistemas democráticos de la Unión e impidan la desinformación en el período previo a las próximas elecciones, la Unión ha realizado avances considerables hacia una actuación más coordinada en materia de resiliencia electoral. No obstante, habida cuenta de la brevedad del plazo disponible para garantizar la preparación de la Unión antes de que los votantes europeos acudan a las urnas en mayo de 2019, la Comisión insta a todos los agentes implicados —las autoridades gubernamentales, los partidos políticos y, en particular, las plataformas en línea— a que redoblen los esfuerzos destinados a aumentar la resiliencia electoral para contrarrestar la desinformación. Con vistas a la próxima reunión que el Consejo Europeo celebrará los días 21 y 22 de marzo de 2019, en la que se analizarán los avances logrados en este ámbito, la Comisión insta también a los Estados miembros a reforzar su coordinación para hacer frente a la desinformación y garantizar la protección de las elecciones al Parlamento Europeo.

La UE ha avanzado considerablemente en la senda hacia una Unión de la Seguridad genuina y efectiva, y en particular se ha alcanzado un acuerdo sobre distintas iniciativas legislativas prioritarias que mejorarán la seguridad de toda la ciudadanía. En los últimos meses[1], el Parlamento Europeo y el Consejo han llegado a un acuerdo sobre la interoperabilidad de los sistemas de información de la UE para la gestión de la seguridad, las fronteras y la migración, así como sobre las nuevas normas de la UE para restringir el perímetro de actuación de los terroristas y los delincuentes, dificultando su acceso a los precursores de explosivos, la financiación de sus actividades y sus desplazamientos no detectados. Con el acuerdo alcanzado sobre quince de las veintidós iniciativas legislativas presentadas por la Comisión en el marco de la Unión de la Seguridad (todas ellas figuran en la lista incluida en el anexo I), la UE está cumpliendo lo prometido en un ámbito prioritario conjunto para el Parlamento Europeo, el Consejo y la Comisión[2].

Sin embargo, es necesario realizar esfuerzos adicionales. En particular, en el marco de la actual legislatura, los colegisladores deben abordar la amenaza urgente que representan los contenidos terroristas en línea, llegando a un acuerdo sobre la propuesta de la Comisión. El Parlamento Europeo y el Consejo también deben alcanzar un acuerdo sobre la propuesta que ha presentado la Comisión con objeto de reforzar la Guardia Europea de Fronteras y Costas para aumentar la protección de las fronteras exteriores de la Unión en aras de una mayor

[1] Se amplían así los avances ya realizados en la senda hacia una Unión de la Seguridad genuina y efectiva. Para una panorámica completa, véanse los informes de situación anteriores sobre la Unión de la Seguridad: https://ec.europa.eu/home-affairs/what-we-do/policies/european-agenda-security/legislative-documents_en.

[2] Véase la Declaración conjunta sobre las prioridades legislativas de la UE para el periodo 2018-2019: https://ec.europa.eu/commission/sites/beta-political/files/joint-declaration-eu-legislative-priorities-2018-19_en.pdf.

seguridad.

Los trágicos acontecimientos ocurridos el 15 de marzo de 2019 en Christchurch, Nueva Zelanda, hacen patente el inequívoco e inmediato peligro que sigue suponiendo la amenaza del terrorismo, con independencia de que venga impulsado por la ultraderecha u otras ideologías extremistas. Las dificultades encontradas al tratar de eliminar contenidos transmitidos en directo desde las plataformas de internet y evitar su posterior reaparición subrayan la vital importancia que reviste la propuesta de la Comisión sobre los contenidos terroristas en línea. Es fundamental que las normas propuestas para la eliminación de los contenidos terroristas en línea sean acordadas por los colegisladores con carácter de urgencia. Es igualmente importante, para luchar contra el terrorismo en todas sus formas, que todos los Estados miembros apliquen plenamente la legislación que la UE ha adoptado, sobre todo en respuesta a los atentados terroristas en Europa, a fin de restringir el perímetro de actuación de los terroristas, en particular las Directivas sobre la lucha contra el terrorismo y sobre el control de la adquisición y tenencia de armas de fuego. En el contexto de la lucha contra el extremismo, la Comisión también ha trabajado activamente y ha adoptado medidas pertinentes contra la incitación ilegal al odio en internet, el odio contra los musulmanes y el antisemitismo.

En el presente informe se exponen también los avances realizados en la aplicación de otros expedientes prioritarios en materia de seguridad, en particular en relación con las medidas destinadas a reforzar la protección de los espacios públicos. La ejecución completa y adecuada de las medidas acordadas reviste la máxima prioridad para poder sacar el máximo partido de una Unión de la Seguridad genuina y efectiva. La Comisión está apoyando activamente a los Estados miembros, en particular concediéndoles financiación y facilitando el intercambio de buenas prácticas. Cuando procede, la Comisión hace también 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 acciones por infracción.

La conmemoración del decimoquinto Día europeo de las víctimas del terrorismo el 11 de marzo de 2019, quince años después de los atentados que sacudieron Madrid el 11 de marzo de 2004 y tres años después de los mortíferos atentados acaecidos en Bruselas y Zaventem el 22 de marzo de 2016, es el telón de fondo del presente informe. Prestar apoyo a las víctimas de los atentados terroristas es una parte importante de la labor en pos de una Unión de la Seguridad genuina y efectiva. Para intensificar este apoyo, el 31 de enero de 2019 la Comisión adoptó una Decisión relativa a la financiación de un proyecto piloto centrado en la creación de un centro de asesoramiento de la UE para las víctimas del terrorismo[3]». Dicho organismo actuará como centro de conocimientos especializados y plataforma para los profesionales que se ocupan de las víctimas del terrorismo.

La Comisión acoge con satisfacción la contribución del Informe del Parlamento Europeo sobre las conclusiones y recomendaciones de la Comisión Especial sobre el Terrorismo[4], que constituye una valiosa aportación a la labor conjunta en pos de una Unión de la Seguridad genuina y efectiva.

II. CUMPLIMIENTO DE LAS PRIORIDADES LEGISLATIVAS

[3] C (2019)636 de 31.1.2019.

[4] Resolución del Parlamento Europeo, de 12 de diciembre de 2018, sobre las conclusiones y recomendaciones de la Comisión Especial sobre Terrorismo [2018/2044 (INI)].

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

El intercambio de información es un aspecto central del apoyo que la UE presta a las autoridades nacionales en la lucha contra el terrorismo y la delincuencia grave. A este respecto, la interoperabilidad de los sistemas de información a escala de la UE supone un cambio radical en la forma en que se facilitan los datos a las autoridades nacionales y garantiza que los datos sean exactos y completos. Los colegisladores han alcanzado un acuerdo político sobre las correspondientes propuestas legislativas prioritarias para lograr la **interoperabilidad de los sistemas de información de la UE** en materia de gestión de la seguridad, las fronteras y la migración[5]. Las medidas propuestas permitirán que los sistemas de información de la UE puedan sumar sus fuerzas de forma más inteligente y precisa, respetando plenamente los derechos fundamentales. Al permitir aprovechar al máximo los datos disponibles, la interoperabilidad colmará las lagunas de información y eliminará los ángulos muertos, ayudando a detectar los casos de identidades múltiples y contrarrestar las usurpaciones de identidad. Una vez que los colegisladores adopten formalmente las nuevas normas, la Comisión podrá prestar apoyo a los Estados miembros en su aplicación. Es necesaria una cooperación estrecha con las agencias de la UE y todos los Estados miembros y países asociados de Schengen para alcanzar el ambicioso objetivo de lograr la plena interoperabilidad de los sistemas de información de la UE a efectos de la gestión de la seguridad, las fronteras y la migración de aquí a 2020. Como preparación para ello, el 5 de marzo de 2019 se celebró un primer seminario con expertos de los Estados miembros para emprender un proceso de coordinación eficaz.

Por ahora, la futura estructura de los sistemas interoperables de información de la UE incluirá el **Sistema de Información Schengen**[6] reforzado, el **Sistema de Información de Visados**[7] existente, la recientemente aprobada extensión del **Sistema Europeo de Información de Antecedentes Penales**[8] a los nacionales de terceros países y los recientemente establecidos **Sistema de Entradas y Salidas de la UE**[9] y **Sistema Europeo de Información y Autorización de Viajes (SEIAV)**[10].

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 de modificación técnica del Reglamento correspondiente[11]. Los cambios propuestos se refieren a los actos jurídicos de los sistemas de información de la UE que el Sistema Europeo de Información y Autorización de Viajes podrá consultar en el marco de la evaluación de los riesgos de seguridad o migración

---

5 COM (2017) 793 final de 12.12.2017, COM (2017) 794 final de 12.12.2017, COM (2018) 478 final de 13.6.2018 y COM (2018) 480 final de 13.6.2018. El acuerdo político alcanzado el 5 de febrero de 2019 fue aprobado por el Comité de Representantes Permanentes del Consejo el 13 de febrero de 2019 y por la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo el 19 de ese mismo mes.

6 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.

7 Reglamento (CE) 767/2008 de 9.7.2008.

8 Los colegisladores alcanzaron un acuerdo político sobre esta propuesta prioritaria el 11 de diciembre de 2018 [COM (2017) 344 final de 29.6.2017]. El Comité de Representantes Permanentes del Consejo aprobó el acuerdo el 19 de diciembre de 2018. El Parlamento Europeo confirmó el acuerdo en su sesión plenaria de 11 de marzo de 2019.

9 Reglamento (UE) 2017/2226 de 30.11.2017.

10 Reglamento (UE) 2018/1240 de 12.9.2018 y Reglamento (UE) 2018/1241 de 12.9.2018.

11 COM (2019) 4 final de 7.1.2019.

irregular de los nacionales de terceros países exentos de la obligación de visado antes de su desplazamiento al espacio Schengen. Las modificaciones propuestas son necesarias para completar la configuración del Sistema Europeo de Información y Autorización de Viajes. La Comisión insta a los colegisladores a impulsar su labor sobre las 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.

En mayo de 2018, la Comisión presentó una propuesta para **reforzar el actual Sistema de Información de Visados**[12], 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 en cuanto se constituya el próximo Parlamento Europeo.

En mayo de 2016, la Comisión propuso extender el ámbito de aplicación de **Eurodac**[13], 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[14] y la Comunicación de la Comisión de 6 de marzo de 2019 sobre el avance en la aplicación de la Agenda Europea de Migración[15], la Comisión insta a los colegisladores a proceder sin demora a la adopción de la propuesta legislativa. Su adopción permitirá que Eurodac forme 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 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**, en relación con la cual está próximo un acuerdo, antes de las elecciones al Parlamento Europeo. *(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**.

2. Reforzar la seguridad mejorando la gestión de las fronteras exteriores

Una protección sólida de las fronteras exteriores es una condición previa para la seguridad en el espacio de libre circulación sin controles en las fronteras interiores. Esta tarea corresponde a los Estados miembros, que tienen que garantizar la gestión de sus fronteras exteriores tanto en su propio interés como en el interés común de todos, con la ayuda de la **Guardia Europea de Fronteras y Costas**. En respuesta a las conclusiones del Consejo Europeo de junio de

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

2018[16], en septiembre de 2018 la Comisión propuso reforzar las capacidades de la Guardia Europea de Fronteras y Costas[17]. La Agencia accedería así a un nuevo nivel operativo, al disponer de un cuerpo permanente de 10 000 guardias de fronteras dotados de poderes ejecutivos y equipo propio, que respetaría plenamente los derechos fundamentales y la soberanía de los Estados miembros.

La labor legislativa sobre la propuesta está avanzando adecuadamente y las negociaciones entre los colegisladores han entrado en la fase crucial. El Parlamento Europeo adoptó su mandato de negociación el 11 de febrero de 2019, mientras que el Consejo recibió el suyo el 20 de febrero de 2019. El 27 de febrero y el 12 de marzo de 2019 se celebraron dos reuniones de diálogo tripartito. La Comisión acoge con satisfacción y apoya el avance realizado en este expediente prioritario, que muestra el compromiso adoptado por todas las instituciones para adoptar esta propuesta antes de las elecciones al Parlamento Europeo de 2019.

Con el fin de reforzar la seguridad a través de la mejora de la gestión de las fronteras exteriores, la Comisión insta al Parlamento Europeo y al Consejo a:

- adoptar la propuesta legislativa para reforzar la **Guardia Europea de Fronteras y Costas** durante la legislatura actual del Parlamento Europeo. *(iniciativa presentada en el Discurso sobre el estado de la Unión de 2018)*

3. Prevenir la radicalización

Abordar el problema de los contenidos terroristas en línea sigue siendo un reto clave en la lucha contra el terrorismo y la prevención de la radicalización. Estos contenidos han desempeñado un papel en la mayor parte de los ataques acaecidos en suelo europeo en los dos últimos años, ya sea incitando a perpetrar atentados, ya sea facilitando instrucciones sobre cómo llevarlos a cabo o enalteciendo sus mortíferos resultados. Con el fin de atajar el peligro evidente e inmediato que suponen estos contenidos, el Discurso sobre el estado de la Unión de 2018 del presidente Juncker estuvo acompañado de una propuesta[18] de Reglamento sobre **contenidos terroristas en línea**, en la que se establece un marco jurídico para impedir el uso indebido de los prestadores de servicios de alojamiento de datos para la difusión de contenidos terroristas en línea. Es esencial que las futuras normas prevean medidas eficaces que, sin menoscabo alguno de la libertad de expresión y otros derechos fundamentales, permitan eliminar los contenidos terroristas en línea lo más rápidamente posible, dado que el daño que pueden causar aumenta con cada hora que pasa.

Aunque el Consejo adoptó su mandato de negociación en diciembre de 2018, la tramitación en el Parlamento Europeo aún no ha concluido; es de esperar que le permita aprobar su mandato de negociación en el transcurso de marzo de 2019[19]. La Comisión pide a ambos colegisladores que alcancen un acuerdo sobre la legislación propuesta durante la actual legislatura del Parlamento Europeo, dada la importancia vital de un marco regulador de la UE con normas y salvaguardias claras para la eliminación de los contenidos terroristas en línea.

---

16 https://www.consilium.europa.eu/media/35936/28-euco-final-conclusions-en.pdf.

17 COM(2018) 631 final de 12.9.2018.

18 COM(2018) 640 final de 12.9.2018.

19 La Comisión de Mercado Interior y Protección del Consumidor del Parlamento Europeo votó su dictamen el 4 de marzo de 2019. La Comisión de Cultura y Educación del Parlamento Europeo votó su informe el 11 de marzo de 2019. Se prevé que la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo vote su informe el 21 de marzo de 2019.

Paralelamente, la Comisión sigue prestando apoyo a los Estados miembros en sus esfuerzos por **prevenir la radicalización**. Un mecanismo de cooperación específico de la UE, en el que participan los representantes nacionales, ayuda a garantizar que el apoyo a escala de la UE responde a las necesidades de los Estados miembros[20]. Cabe citar, entre los ejemplos recientes, una conferencia sobre «Las ciudades de la UE contra la radicalización», organizada conjuntamente con el Comité de las Regiones el 26 de febrero de 2019. El 13 de marzo de 2019, la Comisión organizó una reunión de expertos y responsables políticos nacionales a fin de determinar medidas prácticas que permitan aumentar el apoyo dado a los servicios penitenciarios y de libertad vigilada. El resultado de esta labor pasará a formar parte de un manual que la Red para la Sensibilización frente a la Radicalización está elaborando sobre la rehabilitación y la reinserción de los terroristas condenados, los combatientes terroristas extranjeros que retornan a sus países y los presos que se radicalizan en prisión (véase también la sección IV.4).

Para prevenir la radicalización, la Comisión insta al Parlamento Europeo a:

- adoptar, con carácter prioritario, su mandato de negociación sobre la propuesta legislativa encaminada a evitar la difusión de **contenidos terroristas en línea**, a fin de que los colegisladores lleguen a un acuerdo sobre la legislación durante la actual legislatura del Parlamento Europeo. *(iniciativa presentada en el Discurso sobre el estado de la Unión de 2018)*

4. Mejora de la ciberseguridad

Las amenazas cibernéticas clásicas contra los datos y sistemas siguen aumentando, y en 2018 se ha registrado un incremento de la actividad de agentes malintencionados con una amplia gama de objetivos y víctimas. Por lo tanto, el refuerzo de la ciberseguridad y la lucha contra los delitos informáticos siguen siendo ámbitos prioritarios de actuación para la UE. La UE ha realizado avances tangibles en la mejora de su ciberseguridad, aplicando las medidas establecidas en la Comunicación[21] conjunta de septiembre de 2017 titulada «Resiliencia, disuasión y defensa: fortalecer la ciberseguridad de la UE».

El 12 de marzo de 2019, el Parlamento Europeo confirmó en sesión plenaria el acuerdo político alcanzado por los colegisladores en relación con el **Reglamento de Ciberseguridad**. Cuando entre en vigor, en principio en mayo de 2019, las normas en él contempladas aumentarán las capacidades de ciberseguridad y la preparación de los Estados miembros y las empresas. El Reglamento de Ciberseguridad contribuirá a establecer un marco de certificación de ciberseguridad de la UE para los productos, sistemas y servicios de las tecnologías de la información y comunicación. Mejorará también la cooperación y la coordinación entre los Estados miembros y las instituciones, agencias y organismos de la UE, en particular la Agencia de la Unión Europea para la Ciberseguridad.

No obstante, es necesario seguir avanzando en la propuesta presentada por la Comisión en septiembre de 2018, relativa al **Centro Europeo de Competencia Industrial, Tecnológica y**

[20] Las necesidades de los Estados miembros en materia de prevención de la radicalización se han precisado, por primera vez, en las denominadas orientaciones estratégicas para las acciones preventivas de la UE durante 2019. Esas orientaciones estratégicas pueden consultarse en la siguiente dirección: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3626&news=1&mod_groups=1&month=08&year=2018.

[21] JOIN(2017) 450 final de 13.9.2017.

de Investigación en Ciberseguridad y la **Red de Centros Nacionales de Coordinación**[22]. La propuesta tiene por objeto apoyar las capacidades tecnológicas e industriales de ciberseguridad y aumentar la competitividad de la industria de la ciberseguridad en la Unión. El Parlamento Europeo y el Consejo adoptaron sus mandatos de negociación el 13 de marzo de 2019, fecha en la que tuvo también lugar la primera reunión tripartita. La Comisión insta a los colegisladores a alcanzar rápidamente un acuerdo sobre la legislación propuesta.

La UE ha realizado un significativo avance para precisar los dispositivos prácticos de la respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas (el «conjunto de instrumentos de ciberdiplomacia»), atendiendo al llamamiento realizado por el Consejo Europeo[23] para impulsar la labor de mejora de la capacidad de respuesta ante ciberataques y su disuasión mediante medidas restrictivas de la UE. El 8 de marzo de 2019, la Comisión y la alta representante de la Unión para Asuntos Exteriores y Política de Seguridad presentaron una propuesta conjunta de Reglamento del Consejo con medidas restrictivas para luchar contra los ciberataques de que pueden ser objeto la Unión o sus Estados miembros. La Comisión y la alta representante instan a la rápida adopción de esta propuesta para reforzar la resiliencia de la Unión frente a los ciberataques.

Con el fin de reforzar la ciberseguridad, la Comisión y la alta representante instan al Consejo a:

- adoptar el Reglamento del Consejo relativo a la adopción de **medidas restrictivas contra los ciberataques** que amenazan a la Unión o a sus Estados miembros.

5. Restringir el perímetro de actuación de los terroristas

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, la financiación de sus actividades y sus desplazamientos no detectados.

El 14 de febrero de 2019, el Parlamento Europeo y el Consejo alcanzaron un acuerdo político sobre la propuesta de Reglamento relativo a **restricciones de la comercialización y la utilización de precursores de explosivos**[24]. Una vez que sea aplicable, el Reglamento introducirá mejoras significativas en el actual marco legislativo, limitando el acceso a los precursores de explosivos peligrosos que podrían utilizarse indebidamente para fabricar artefactos explosivos artesanales. Colmará lagunas en materia de seguridad con medidas tales como la prohibición de otras sustancias químicas, la comprobación obligatoria de los registros de antecedentes penales de quienes soliciten un permiso de compra de sustancias restringidas y la aclaración de que las normas aplicables a los operadores económicos también se aplican a las empresas que operan en línea.

Además, en el marco de los esfuerzos de lucha contra la financiación del terrorismo, los colegisladores llegaron a un acuerdo sobre la propuesta de Directiva para **facilitar el uso de información financiera y de otro tipo** a efectos de prevención, detección, investigación y enjuiciamiento de los delitos graves[25]. Una vez adoptada formalmente y aplicada, la Directiva

[22] COM(2018) 630 final de 12.9.2018.
[23] Véanse las conclusiones del Consejo Europeo de junio y octubre de 2018.
[24] COM(2018) 209 final de 17.4.2018.
[25] Los colegisladores alcanzaron un acuerdo político sobre la propuesta de la Comisión el 12 de febrero de 2019 [COM(2018) 213 final de 17.4.2018]. La propuesta fue aprobada por el Comité de Representantes

proporcionará a los servicios de seguridad designados y a los organismos de recuperación de activos un acceso directo a la información sobre cuentas bancarias incluida en los registros nacionales centralizados de cuentas bancarias. La Directiva mejorará también la cooperación entre las Unidades de Información Financiera nacionales y las autoridades con funciones coercitivas, y facilitará el acceso de Europol a la información financiera.

Basándose en todo ello, la Comisión seguirá reflexionando sobre la cooperación entre las Unidades de Información Financiera de los distintos Estados miembros, en particular en el próximo informe sobre la cooperación entre las Unidades de Información Financiera, según lo previsto en la quinta Directiva contra el blanqueo de capitales[26]. Además, como también se exige en esa norma, la Comisión está evaluando los aspectos relacionados con la posible interconexión de los registros nacionales centralizados de cuentas bancarias y los sistemas de recuperación de datos en la UE. La Comisión está analizando asimismo las medidas de decomiso no basado en condena en la Unión. Por último, y también en respuesta al llamamiento del Parlamento Europeo[27], la Comisión seguirá evaluando la necesidad, la viabilidad técnica y la proporcionalidad de medidas adicionales para rastrear la financiación del terrorismo en la UE.

Como parte de la lucha contra el fraude documental, el 19 de febrero de 2019 los colegisladores llegaron a un acuerdo provisional en relación con la propuesta de Reglamento sobre el refuerzo de la **seguridad de las tarjetas de identidad de los ciudadanos de la Unión y de los documentos de residencia**[28] para que no puedan ser utilizados fraudulentamente por delincuentes o terroristas. La Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo refrendó el acuerdo el 11 de marzo de 2019. Una vez adoptado, el Reglamento introducirá medidas mínimas de seguridad para las tarjetas de identidad, incluidos identificadores biométricos (una imagen facial y dos impresiones dactilares) en un chip sin contacto. Con ello se mejorará significativamente la seguridad de los documentos de identidad y de residencia nacionales y se dificultará que los terroristas y otros delincuentes puedan hacer un uso fraudulento de dichos documentos o falsificarlos con objeto de entrar en la UE o desplazarse por ella. El aumento de la seguridad de los documentos de identidad contribuirá a reforzar la gestión de las fronteras exteriores de la UE. Al mismo tiempo, el incremento de la seguridad y fiabilidad de los documentos facilitará el ejercicio del derecho a la libre circulación de los ciudadanos de la UE.

No obstante, es necesario seguir avanzando en las propuestas de la Comisión de abril de 2018 sobre el **acceso a las pruebas electrónicas**, dado que más de la mitad de todas las investigaciones judiciales en la actualidad implican una solicitud transfronteriza de acceso a

---

Permanentes del Consejo el 20 de febrero de 2019 y por la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo el 26 de ese mismo mes.

[26] El artículo 65, apartado 2, de la Directiva (UE) 2018/843 (19.6.2018) establece que, a más tardar el 1 de junio de 2019, la Comisión evaluará el marco de la cooperación de las Unidades de Información Financiera con terceros países y los obstáculos y oportunidades para mejorar la cooperación entre las Unidades de Información Financiera en la Unión, incluida la posibilidad de establecer un mecanismo de coordinación y apoyo.

[27] 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.

[28] COM(2018) 212 final de 17.4.2018.

pruebas electrónicas[29]. El Consejo adoptó su mandato de negociación sobre las propuestas de Reglamento[30] para mejorar el acceso transfronterizo a las pruebas electrónicas en las investigaciones judiciales y de Directiva[31] por la que se establecen normas armonizadas sobre el nombramiento de representantes legales a efectos de recabar pruebas para procesos penales. Sin embargo, en el Parlamento Europeo apenas ha habido avances en relación con las propuestas desde su aprobación por la Comisión en abril de 2018. Dada la importancia crucial que reviste el acceso eficiente a las pruebas electrónicas para el enjuiciamiento de delitos transfronterizos tales como el terrorismo o la ciberdelincuencia, la Comisión insta al Parlamento Europeo a avanzar en esta labor.

Paralelamente, la Comisión está trabajando en sus **iniciativas internacionales sobre el acceso a las pruebas electrónicas** en el marco de las negociaciones en curso con los Estados Unidos y sobre un segundo Protocolo adicional del Convenio sobre Ciberdelincuencia del Consejo de Europa (Convenio de Budapest). Por lo tanto, el 5 de febrero de 2019, la Comisión aprobó sendas recomendaciones[32] sobre los mandatos de negociación para ambas iniciativas internacionales. Los proyectos de mandato se debatieron en la reunión del Consejo de Justicia y Asuntos de Interior celebrada los días 7 y 8 de marzo de 2019, pero las discusiones aún no han concluido en el Consejo. La Comisión pide al Consejo que adopte la Decisión por la que se autoriza la participación en las negociaciones para un segundo Protocolo adicional del Convenio sobre Ciberdelincuencia del Consejo de Europa (Convenio de Budapest), así como la Decisión por la que se autoriza la apertura de negociaciones con los Estados Unidos sobre el acceso transfronterizo a las pruebas electrónicas. Es importante emprender rápidamente las negociaciones para impulsar la cooperación internacional en materia de intercambio de pruebas electrónicas, garantizando al mismo tiempo la compatibilidad con el Derecho de la UE y las obligaciones de los Estados miembros en virtud del mismo, teniendo también en cuenta la futura evolución de la legislación de la UE.

Con el fin de restringir el perímetro de actuación de los terroristas, la Comisión pide:

- que el Parlamento Europeo adopte con carácter de urgencia su mandato de negociación para las propuestas legislativas sobre las pruebas electrónicas a fin de entablar sin demora los debates tripartitos con el Consejo; *(prioridad de la Declaración conjunta)*
- que el Consejo adopte la Decisión por la que se autoriza la participación en las negociaciones para un **segundo Protocolo adicional del Convenio sobre Ciberdelincuencia del Consejo de Europa (Convenio de Budapest),** y que autorice la apertura de **negociaciones con los Estados Unidos** sobre el acceso transfronterizo a las pruebas electrónicas.

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

[29] 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].

[30] 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.

[31] COM(2018) 226 final de 17.4.2018. El Consejo adoptó su mandato de negociación sobre la propuesta de Directiva en el Consejo de Justicia y Asuntos de Interior celebrado el 8 de marzo de 2019.

[32] COM (2019) 70 final de 5.2.2019 y COM (2019) 71 final de 5.2.2019.

La capacidad de agentes internos y externos para interferir en los debates públicos y manipular las elecciones nunca ha sido más real y aún podría aumentar más en la perspectiva de las próximas elecciones al Parlamento Europeo. Las posibles consecuencias —la socavación o deslegitimación de las instituciones democráticas— constituyen una amenaza grave, de carácter estratégico y cada vez mayor. Son una parte esencial de los retos en materia de seguridad a que se enfrenta actualmente la UE, que rebasan las fronteras nacionales y requieren una respuesta transfronteriza conjunta.

Las campañas electorales previas a las elecciones al Parlamento Europeo comenzarán en serio en marzo. Antes del Consejo Europeo de los días 21 y 22 de marzo de 2019, la Comisión insta a los Estados miembros a intensificar su labor de coordinación e intercambio de información para contrarrestar la desinformación y proteger las elecciones contra las amenazas cibernéticas. Los Estados miembros deben hacer pleno uso de las herramientas y los canales de información que brinda la UE, en particular el Sistema de Alerta Rápida[33] recientemente establecido. Por otra parte, debido a la preocupación que suscita el estado actual de la situación, la Comisión insta a las plataformas en línea a acelerar sus esfuerzos en todos los Estados miembros para contribuir a garantizar la integridad de las elecciones al Parlamento Europeo de mayo de 2019.

Para apoyar y fomentar estos esfuerzos, la Comisión y la alta representante siguen tomando medidas centradas en dos ámbitos complementarios a fin de dar respuesta a las amenazas cibernéticas: contrarrestar la desinformación y mejorar la resiliencia electoral.

1. Adopción de medidas contra la desinformación

La exposición de la ciudadanía a la desinformación masiva, incluida la información engañosa o abiertamente falsa, puede constituir un tipo de amenaza cibernética grave y supone un importante desafío de cara a las próximas elecciones europeas. La Comisión está supervisando de cerca la aplicación de las medidas expuestas en su **Comunicación sobre la lucha contra la desinformación en línea**[34]**, de abril de 2018**.

Por otra parte, los avances realizados en el marco del Código de Buenas Prácticas sobre Desinformación, firmado en octubre de 2018 por representantes de las plataformas en línea, las principales redes sociales, el sector de la publicidad y los propios anunciantes, son objeto de un estrecho seguimiento por parte de la Comisión (*cf. infra*). La Comisión llevará a cabo una evaluación global tras los primeros doce meses de aplicación del Código. Si su aplicación y sus efectos resultaran insatisfactorios, la Comisión podría proponer nuevas medidas, incluso de carácter legislativo.

Partiendo de esta labor, y respondiendo al llamamiento realizado por el Consejo Europeo de junio de 2018 para que se protegieran los sistemas democráticos de la Unión, la Comisión y la alta representante presentaron un **Plan de Acción Conjunto contra la Desinformación**[35] en

[33] Enmarcado en el plan de acción contra la desinformación presentado por la Comisión y la alta representante en diciembre de 2018 (*cf. infra*), el Sistema de Alerta Rápida será un dispositivo que permitirá a los Estados miembros, las instituciones de la UE y sus socios compartir información sobre las campañas de desinformación en curso y coordinar sus respuestas. El Sistema se basará únicamente en información de código abierto y no clasificada.

[34] COM(2018) 236 final de 26.4.2018, seguida de un informe de aplicación [COM(2018) 794 final de 5.12.2018].

[35] JOIN (2018) 36 final de 5.12.2018.

diciembre de 2018. En él se destaca que, según la **Célula de Fusión de la UE contra las Amenazas Híbridas**, la desinformación procedente de la Federación de Rusia supone la mayor amenaza para la Unión, pues es sistemática, cuenta con muchos recursos y es de una dimensión no comparable a la de otros países. Para hacer frente a la amenaza que supone la desinformación, el Plan de Acción prevé un aumento de los recursos destinados a luchar contra ella, más concretamente por lo que se refiere a los **Grupos Especiales sobre Comunicación Estratégica** del Servicio Europeo de Acción Exterior (SEAE), incluido el Grupo de Trabajo East StratCom[36]. El Plan de Acción también prevé un aumento de los recursos destinados a este ámbito, y reclama su incremento adicional a lo largo de los dos próximos años.

El Plan de Acción establece medidas concretas para combatir la desinformación, incluida la creación de un **Sistema de Alerta Rápida**. En la perspectiva de las elecciones al Parlamento Europeo, en marzo de 2019 se ha creado dicho Sistema de Alerta Rápida para facilitar el intercambio de datos entre los Estados miembros y las instituciones de la UE y la evaluación de las campañas de desinformación e instar a la vigilancia sobre las amenazas en este ámbito.

El Plan de Acción también prevé un estrecho seguimiento de la aplicación del Código antes mencionado que han firmado las plataformas en línea. El 29 de enero de 2019, la Comisión publicó los **informes presentados por los firmantes del Código de Buenas Prácticas** (Google, Facebook, Twitter, Mozilla y las asociaciones profesionales del sector de la publicidad). Aunque la Comisión acogió con satisfacción los progresos realizados, también instó a los firmantes a intensificar sus esfuerzos en el período previo a las elecciones al Parlamento Europeo de 2019[37].

El 28 de febrero de 2019, la Comisión publicó los **informes de Facebook, Google y Twitter** sobre los avances realizados en enero de 2019 en sus compromisos de lucha contra la desinformación. Los datos en ellos facilitados no permiten concluir que las nuevas políticas y herramientas se estén aplicando de manera tempestiva y con recursos suficientes en los distintos Estados miembros. Es evidente que hay margen de mejora por parte de todos los signatarios[38]. Más concretamente, la Comisión pide a las plataformas que garanticen la transparencia de los anuncios políticos antes del inicio de la campaña de las elecciones europeas en todos los Estados miembros de la UE, que permitan un acceso adecuado a sus datos a efectos de investigación y comprobación, y que garanticen una cooperación apropiada con los distintos Estados miembros a través de los puntos de contacto del Sistema de Alerta Rápida.

El 20 de marzo de 2019, la Comisión presentará un nuevo informe sobre la aplicación del citado Código de Buenas Prácticas.

2. Mejora de la resiliencia electoral

El 12 de septiembre de 2018, la Comisión adoptó una batería de medidas para mejorar la resiliencia de los sistemas electorales dirigidas a los Estados miembros y las fundaciones y los

---

[36] Desde su creación en 2015, el Grupo de Trabajo East StratCom ha catalogado, analizado y puesto en el punto de mira cerca de 5 000 ejemplos de desinformación procedente de la Federación de Rusia, revelando numerosos relatos ficticios, exponiendo las herramientas, técnicas e intenciones de las campañas de desinformación y sensibilizando sobre ellas.

[37] Para más información, véase: http://europa.eu/rapid/press-release_IP-19-746_en.htm.

[38] Para más información, véase: http://europa.eu/rapid/press-release_STATEMENT-19-1379_en.htm.

partidos políticos europeos y nacionales, en particular una Recomendación sobre las redes de cooperación electoral, la transparencia en línea, la protección contra los incidentes de ciberseguridad y la lucha contra las campañas de desinformación, orientaciones sobre la aplicación de la legislación de la UE en materia de protección de datos[39] y una modificación legislativa destinada a endurecer las normas que rigen la financiación de los partidos políticos europeos.

El Parlamento Europeo acogió con satisfacción la batería de medidas en la Resolución que adoptó el 28 de octubre de 2018. El Consejo acogió favorablemente esas medidas en sus Conclusiones de 19 de febrero de 2019 sobre la garantía de unas elecciones europeas libres y justas, que expresen el compromiso común de todos los Estados miembros con un enfoque europeo coordinado capaz de preservar la integridad de los próximos comicios europeos. El Consejo de Justicia y Asuntos de Interior debatió el estado de la cuestión el 7 de marzo de 2019.

La modificación del Reglamento sobre el **estatuto y la financiación de los partidos y fundaciones políticos europeos**[40] introduce la posibilidad de imponer sanciones por el uso ilegal de datos personales en caso de impacto deliberado sobre el resultado de las elecciones al Parlamento Europeo. Tras el acuerdo político[41] alcanzado en enero de 2019, el Parlamento Europeo reunido en sesión plenaria, aprobó el texto de la enmienda el 12 de marzo de 2019. Está previsto que la modificación se incorpore a la legislación antes de las elecciones al Parlamento Europeo de 2019.

La Recomendación sobre **las redes de cooperación electoral, la transparencia en línea, la protección contra los incidentes de ciberseguridad y la lucha contra las campañas de desinformación en el contexto de las elecciones al Parlamento Europeo**[42] va dirigida a los Estados miembros y a las fundaciones y partidos políticos nacionales y europeos, y presenta medidas concretas para los agentes pertinentes en esos ámbitos. En aras de su aplicación, las redes electorales nacionales designaron puntos de contacto para participar en una **red de cooperación europea en materia de elecciones** que permita instar a la vigilancia sobre amenazas, intercambiar buenas prácticas, debatir soluciones comunes para los retos concretos y fomentar proyectos y ejercicios impulsados conjuntamente por las redes nacionales. En la primera reunión de la red, celebrada el 21 de enero de 2019, los participantes coincidieron en la importancia de adoptar un enfoque global que permita garantizar la integridad de las elecciones sin menoscabo del debate democrático abierto y la igualdad de condiciones en la esfera política. La segunda reunión se celebró el 27 de febrero de 2019 y se centró en el seguimiento y la aplicación de aspectos relacionados con el contexto electoral, por ejemplo la protección de datos, la regulación de los medios de comunicación, la garantía del cumplimiento de la legislación, la transparencia y los medios sociales de comunicación y la participación de los distintos agentes en las actividades de seguimiento. La reunión ha sentado las bases para que los participantes puedan tomar parte en un ejercicio de ciberresiliencia inmediatamente después de la próxima reunión de la red, prevista para el 5 de abril de 2019.

---

39 COM(2018) 638 final de 12.9.2018.

40 COM(2018) 636 final de 12.9.2018.

41 El acuerdo político que alcanzaron los colegisladores el 16 de enero de 2019 fue refrendado por el Comité de Representantes Permanentes del Consejo el 25 de enero de 2019 y por la Comisión de Libertades Civiles, Justicia y Asuntos de Interior del Parlamento Europeo el 29 de enero de 2019.

42 C(2018) 5949 final de 12.9.2018.

El 19 de febrero de 2019 se celebró un **seminario sobre las modalidades prácticas para reforzar la ciberresiliencia de las elecciones**, organizado conjuntamente por el Parlamento Europeo y la Comisión, a fin de mejorar la seguridad y la resiliencia de los sistemas y las infraestructuras electorales frente a la constante evolución de las amenazas cibernéticas. Las autoridades nacionales responsables de ciberseguridad en los Estados miembros, la Agencia de Seguridad de las Redes y de la Información de la Unión Europea y las plataformas en línea debatieron medidas centradas en actuaciones urgentes y pertinentes para garantizar la integridad de las elecciones al Parlamento Europeo de 2019.

Las instituciones de la UE y los Estados miembros también cooperan estrechamente en otras **actividades de sensibilización** destinadas a proteger la integridad del proceso electoral y a implicar a los agentes públicos y privados, incluidos los medios de comunicación, las plataformas en línea y la sociedad civil.

Para hacer frente a la desinformación y garantizar la resiliencia electoral, la Comisión y la alta representante instan a los Estados miembros a:

- poner en práctica rápidamente y de manera decidida las actuaciones contempladas en el **Plan de Acción Conjunto contra la Desinformación** de diciembre de 2018.

IV. OTRAS CUESTIONES PRIORITARIAS EN MATERIA DE SEGURIDAD

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

La ejecución completa y correcta de las medidas acordadas reviste la máxima prioridad para garantizar el pleno beneficio de una Unión de la Seguridad genuina y efectiva. La Comisión está apoyando activamente a los Estados miembros, en particular concediéndoles financiación y facilitando el intercambio de buenas prácticas. Cuando procede, la Comisión también hace 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 acciones por infracción.

Por lo que respecta a la aplicación de la **Directiva de la UE relativa al registro de los nombres de los pasajeros**[43], el 19 de julio de 2018 la Comisión inició procedimientos de infracción contra catorce Estados miembros por no haber comunicado la adopción de la legislación nacional de transposición de la Directiva[44], que constituye un instrumento fundamental en la lucha contra el terrorismo y los delitos graves. Desde entonces, nueve de ellos han notificado su plena transposición[45]. Los Estados miembros en los que aún no se ha completado la transposición han recibido dictámenes motivados (España, el 24 de enero de 2019, los Países Bajos y Finlandia el 7 de marzo de 2019). 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**[46] expiró el 8 de septiembre de 2018. El 22 de noviembre de 2018, la Comisión inició procedimientos de

43 Directiva (UE) 2016/681 de 27.4.2016.

44 Bulgaria, Chequia, Estonia, Grecia, España, Francia, Chipre, Luxemburgo, Países Bajos, Austria, Portugal, Rumanía, Eslovenia y Finlandia.

45 Bulgaria, Estonia, Grecia, Francia, Chipre, Luxemburgo, Austria, Portugal y Rumanía (situación a 11 de marzo de 2019).

46 Directiva (UE) 2017/541 de 15.3.2017.

infracción contra dieciséis Estados miembros por no haber comunicado la adopción de la legislación nacional de transposición plena de la Directiva. Desde entonces, nueve de ellos han notificado su plena transposición[47]. La Comisión insta a los otros siete a adoptar las medidas necesarias lo antes posible[48].

El plazo para la transposición de la **Directiva sobre el control de la adquisición y tenencia de armas**[49] expiró el 14 de septiembre de 2018. Hasta la fecha, seis Estados miembros han notificado la transposición plena[50] y cinco la transposición parcial[51]. El 22 de noviembre de 2018 veintidós Estados miembros[52], incluidos los que han notificado la transposición parcial, recibieron cartas de emplazamiento de la Comisión.

Por lo que se refiere a la transposición al Derecho nacional de la **Directiva sobre protección de datos en el ámbito penal**[53], el 19 de julio de 2018 la Comisión inició procedimientos de infracción contra diecinueve Estados miembros por falta de comunicación de la adopción de la legislación nacional que garantice la plena transposición de la Directiva[54]. Por el momento, diecisiete Estados miembros han notificado la transposición plena y cinco la transposición parcial[55]. Hasta la fecha se han archivado los procedimientos contra seis Estados miembros[56], mientras que nueve Estados miembros recibieron un dictamen motivado el 25 de enero de 2019[57].

Está previsto que la Comisión informe sobre la coherencia de la identificación de los operadores de servicios esenciales antes del 9 de mayo de 2019. A la luz de las notificaciones de los Estados miembros, se ha establecido que la Directiva sobre la seguridad de las redes y los sistemas de información[58] se ha transpuesto en su totalidad en veinticinco Estados miembros y parcialmente en un Estado miembro[59]. En enero de 2019, la Comisión archivó los

---

47 Bulgaria, Chequia, Alemania, Estonia, España, Francia, Croacia, Italia, Letonia, Lituania, Hungría, Malta, Países Bajos, Austria, Portugal, Eslovaquia, Finlandia y Suecia notificaron la transposición plena (situación a 11 de marzo de 2019).

48 Bélgica, Polonia, Rumanía y Eslovenia han notificado la transposición parcial. Grecia, Chipre y Luxemburgo no han remitido ninguna notificación (situación a 11 de marzo de 2019).

49 Directiva (UE) 2017/853 de 17.5.2017.

50 Dinamarca, Francia, Croacia, Italia, Malta y Austria (situación a 11 de marzo de 2019).

51 Chequia, Estonia, Lituania, Portugal y Reino Unido (situación a 11 de marzo de 2019).

52 Bélgica, Bulgaria, Chequia, Alemania, Estonia, Irlanda, Grecia, España, Chipre, Letonia, Lituania, Luxemburgo, Hungría, Países Bajos, Polonia, Portugal, Rumanía, Eslovenia, Eslovaquia, Finlandia, Suecia y Reino Unido (situación a 11 de marzo de 2019).

53 Directiva (UE) 2016/680 de 27.4.2016.

54 Bélgica, Bulgaria, Chequia, Estonia, Grecia, España, Francia, Croacia, Chipre, Letonia, Lituania, Luxemburgo, Hungría, Países Bajos, Polonia, Portugal, Rumanía, Eslovenia y Finlandia. La Comisión está recibiendo y analizando las respuestas de los Estados miembros, incluidas las notificaciones de la legislación correspondiente (situación a 11 de marzo de 2019).

55 Bélgica, Alemania, Estonia, Irlanda, Francia, Croacia, Italia, Lituania, Luxemburgo, Hungría, Malta, Austria, Polonia, Rumanía, Eslovaquia, Suecia y Reino Unido notificaron la plena transposición. Chequia, Portugal, Finlandia, Eslovenia y Países Bajos notificaron la transposición parcial. Dinamarca también ha completado la transposición (situación a 11 de marzo de 2019).

56 Bélgica, Francia, Croacia, Lituania, Luxemburgo y Hungría (situación a 11 de marzo de 2019).
Grecia, Chipre, España, Eslovenia, Portugal, Chequia, Bulgaria, Letonia y Países Bajos (situación a 11 de marzo de 2019).

58 Directiva (UE) 2016/1148 de 27.4.2016.

59 Bulgaria, Chequia, Dinamarca, Alemania, Grecia, Estonia, Irlanda, España, Francia, Croacia, Italia, Chipre, Letonia, Lituania, Malta, Países Bajos, Austria, Polonia, Portugal, Rumanía, Eslovenia, Eslovaquia, Finlandia, Suecia y Reino Unido notificaron la plena transposición. Hungría ha notificado la

procedimientos de infracción por no comunicación incoados contra seis Estados miembros[60]. Nueve Estados miembros[61] están sujetos a un procedimiento de infracción por no comunicación de la plena transposición de la Directiva. En el marco de la transposición de la Directiva sobre la seguridad de las redes y los sistemas de información, los Estados miembros debían presentar a la Comisión, antes del 9 de noviembre de 2018, información sobre los operadores de servicios esenciales identificados en su territorio. La Comisión está evaluando la información presentada por los Estados miembros[62].

Por otra parte, la Comisión está evaluando la transposición de la **cuarta Directiva contra el blanqueo de capitales**[63], trabajando al mismo tiempo para comprobar que los Estados miembros aplican las normas. La Comisión ha incoado procedimientos de infracción contra los veintiocho Estados miembros, pues considera que las comunicaciones que le han remitido no garantizan la transposición plena de la Directiva[64]. La Comisión seguirá utilizando sus facultades cuando proceda para garantizar la plena aplicación de esa Directiva.

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:

- la **Directiva de la UE relativa al registro de los nombres de los pasajeros**, en relación con la cual tres Estados miembros aún no han notificado su incorporación al ordenamiento jurídico nacional y otros dos deben completar la notificación de transposición[65];
- la **Directiva relativa a la seguridad de las redes y los sistemas de información**, en relación con la cual dos Estados miembros aún no han notificado su incorporación al ordenamiento jurídico nacional y otro debe completar la notificación de transposición[66];
- la **Directiva relativa a la lucha contra el terrorismo**, en relación con la cual tres Estados miembros aún no han notificado su incorporación al ordenamiento jurídico nacional y otros cuatro deben completar la notificación sobre su transposición[67];
- la **Directiva sobre el control de la adquisición y tenencia de armas**, en relación con la

transposición parcial. Bélgica y Luxemburgo no han notificado a la Comisión ninguna medida nacional de transposición (situación a 11 de marzo de 2019).

60 Irlanda, España, Francia, Croacia, Países Bajos y Portugal (situación a 11 de marzo de 2019).

61 Bulgaria, Bélgica, Dinamarca, Letonia, Lituania, Luxemburgo, Hungría, Austria y Rumanía (situación a 11 de marzo de 2019).

62 Bulgaria, Chipre, Chequia, Alemania, Dinamarca, Estonia, España, Finlandia, Francia, Croacia, Hungría, Irlanda, Italia, Lituania, Malta, Países Bajos, Polonia, Portugal, Eslovaquia, Suecia y Reino Unido (situación a 11 de marzo de 2019).

63 Directiva (UE) 2015/849 de 20.5.2015.

64 La Comisión ha incoado procedimientos de infracción contra todos los Estados miembros por no comunicar la legislación nacional que transpone plenamente la Directiva, ya que, según su evaluación, ha llegado a la conclusión de que algunas disposiciones de la Directiva no han sido transpuestas.

65 España, Países Bajos y Finlandia todavía no han comunicado la transposición. Chequia y Eslovenia han comunicado una transposición parcial y aún no han completado la notificación de transposición (situación a 11 de marzo de 2019). 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.

66 Bélgica y Luxemburgo todavía no han comunicado la transposición. Hungría ha comunicado una transposición parcial y aún no ha completado la notificación de transposición (situación a 11 de marzo de 2019).

67 Grecia, Chipre y Luxemburgo todavía no han comunicado la transposición. Bélgica, Polonia, Rumanía y Eslovenia han comunicado una transposición parcial y aún no han completado la notificación de transposición (situación a 11 de marzo de 2019).

cual diecisiete Estados miembros aún no han notificado su incorporación al ordenamiento jurídico nacional y otros cinco deben completar la notificación sobre su transposición[68];

- la **Directiva sobre protección de datos en el ámbito penal**, en relación con la cual cinco Estados miembros aún no han notificado su transposición al ordenamiento jurídico nacional y otros cinco deben completar la notificación sobre su transposición[69]; y
- la **cuarta Directiva contra el blanqueo de capitales**, en relación con la cual un Estado miembro aún debe completar la notificación de transposición[70].

2. Protección de los espacios públicos: buenas prácticas recomendadas

Entre las medidas prácticas para mejorar la protección y la resiliencia frente al terrorismo, la Comisión sigue prestando apoyo a los Estados miembros y a sus autoridades locales en **la protección de los espacios públicos**. En aplicación del Plan de Acción de octubre de 2017 para contribuir a la protección de los espacios públicos[71], la labor se centra en el desarrollo y la recopilación de orientaciones y buenas prácticas. Colaborando con las autoridades públicas y los gestores privados de espacios públicos en el denominado Foro de Operadores[72], la Comisión ha identificado una serie de buenas prácticas y medidas que todas las autoridades públicas y gestores involucrados en la protección de los espacios públicos pueden aplicar para aumentar la seguridad[73]. Sientan las bases para orientar la futura labor en todos los sectores pertinentes para la protección de los espacios públicos (véase el recuadro que figura a continuación).

Buenas prácticas para que las autoridades públicas y los operadores privados refuercen la seguridad de los espacios públicos

Evaluación y planificación

68 Bélgica, Bulgaria, Alemania, Irlanda, Grecia, España, Chipre, Letonia, Luxemburgo, Hungría, Países Bajos, Polonia, Rumanía, Eslovenia, Eslovaquia, Finlandia y Suecia aún no han notificado la transposición. Chequia, Estonia, Lituania, Portugal y Reino Unido han comunicado una transposición parcial y aún no han completado la notificación de transposición (situación a 11 de marzo de 2019). 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.

69 Bulgaria, Grecia, España, Chipre y Letonia todavía no han comunicado la transposición. Chequia, Portugal, Países Bajos, Finlandia y Eslovenia han comunicado una transposición parcial y aún no han completado la notificación de transposición (situación a 11 de marzo de 2019).

70 Hasta la fecha, Rumanía solo ha comunicado una transposición parcial y aún no ha completado la notificación de transposición. Todos los demás Estados miembros han notificado la transposición plena. Sin embargo, según la evaluación de la Comisión, sigue habiendo algunas disposiciones de la Directiva cuya transposición no parece haberse completado (situación a 11 de marzo de 2019).

71 COM(2017) 612 final de 18.10.2017.

72 El Foro de Operadores, creado en el marco del Plan de Acción de octubre de 2017 para contribuir a la protección de los espacios públicos, reúne a agentes de los sectores público y privado, en concreto a responsables políticos de los Estados miembros y operadores que intervienen en diferentes sectores, como los espectáculos y acontecimientos de masas, la hostelería, los centros comerciales, deportivos y culturales, las instalaciones de transporte, etc.

73 Para más detalles sobre las buenas prácticas, véase el documento de trabajo de los servicios de la Comisión titulado «Good practices to support the protection of public spaces» [SWD (2019) 140 de 20.3.2019].

- Preparar y llevar a cabo evaluaciones de la vulnerabilidad que permitan detectar posibles puntos vulnerables frente a ataques que puedan perpetrar agentes internos o externos.
- Elaborar y aplicar un plan de seguridad de las instalaciones o el acontecimiento, con medidas de preparación, emergencia y recuperación, en el que se determinen las medidas de seguridad adecuadas teniendo en cuenta todas las circunstancias de las instalaciones o el acontecimiento. Las medidas de seguridad deben ser eficaces, discretas, proporcionadas y ajustadas a las diferentes circunstancias, teniendo en cuenta su funcionamiento específico.
- Designar y formar a una persona responsable de la coordinación y aplicación de las medidas de seguridad incluidas en el plan correspondiente. Y por último:
- Elaborar y aplicar un plan de gestión de crisis.

Sensibilización y formación

- Poner en marcha campañas de sensibilización pública sobre la denuncia de comportamientos sospechosos y la manera de reaccionar en caso de ataque que amenace la seguridad de unas instalaciones o un acontecimiento.
- Desarrollar y aplicar un programa interno de sensibilización en materia de seguridad para todos los empleados.
- Desarrollar y aplicar un programa interno de sensibilización sobre las amenazas por parte de «personas de dentro» que ayude a proteger a las instalaciones o acontecimientos contra diferentes tipos de amenazas, como sabotajes, robos comerciales o atentados terroristas.
- Elaborar programas de formación básica en materia de seguridad para todo el personal e impartir formaciones específicas en la materia, contribuyendo así al desarrollo de una cultura corporativa de seguridad. Desarrollar actividades que motiven a los empleados a aplicar buenas prácticas en materia de seguridad y a mantener un alto nivel de vigilancia. Y por último:
- Realizar ejercicios periódicos de seguridad que ayuden a determinar el nivel de preparación para impedir los atentados o reaccionar ante ellos.

Protección física

- Evaluar las cuestiones de seguridad y protección física desde el inicio del proceso de diseño de una nueva instalación o acontecimiento.
- Evaluar los controles y las barreras de acceso necesarios, evitando al mismo tiempo crear nuevos puntos vulnerables. Los controles y las barreras de acceso no deben desplazar riesgos ni crear nuevos objetivos.
- Evaluar la tecnología más adecuada para la detección de explosivos, armas blancas o de fuego, así como agentes químicos, biológicos, radiológicos o nucleares.

Cooperación

- Designar puntos de contacto y aclarar las funciones y responsabilidades respectivas en la cooperación público-privada en cuestiones de seguridad (por ejemplo, entre los operadores, la seguridad privada y las autoridades policiales y judiciales), también con el objetivo de mejorar la comunicación y la cooperación de manera continua.
- Establecer una comunicación y cooperación fiable y oportuna que permita el intercambio de información sobre riesgos y amenazas específicos entre las autoridades públicas responsables, las autoridades policiales y judiciales y el sector privado.
- Coordinar la labor en materia de protección de los espacios públicos a nivel local, regional y nacional y participar en iniciativas de comunicación e intercambios de buenas prácticas a todos los niveles, incluido el de la UE. Y por último:

- Las autoridades públicas, junto con los operadores, deben desarrollar y facilitar recomendaciones prácticas y guías para detectar, mitigar o responder a las amenazas que pendan sobre la seguridad.

3. Puntos vulnerables de las infraestructuras digitales

La resiliencia digital es crucial para proteger el desarrollo general de la actividad de las administraciones, la investigación industrial, la propiedad intelectual, los planes empresariales, las elecciones, las instituciones democráticas y los propios datos personales. Una de las cuestiones clave en el ámbito de la ciberseguridad que está recibiendo atención generalizada en el debate público en toda la UE es la de las redes de quinta generación (5G). En el reciente Consejo informal de ministros de telecomunicaciones, celebrado en Bucarest el 1 de marzo de 2019 se abogó por un enfoque europeo coordinado para reforzar la resiliencia digital en la UE en relación con esas redes. La infraestructura correspondiente constituye una importante base para la economía digital. Más allá de los servicios prestados a los consumidores, la tecnología 5G se ha diseñado de tal modo que permita prestar servicios esenciales a los sectores verticales, como la movilidad, la energía y la salud. Los estándares de las redes 5G son mundiales, y los equipos y dispositivos serán ofrecidos por una serie de proveedores mundiales.

El despliegue de las redes 5G durante los próximos años supondrá un cambio radical respecto a las redes anteriores. El almacenamiento de datos en la nube permitirá la conexión de miles de millones de dispositivos relacionados con la internet de las cosas y fomentará nuevas innovaciones en el ámbito de la inteligencia artificial, abriendo nuevas oportunidades para los ciudadanos y las empresas. Por lo tanto, la ciberseguridad reviste especial importancia, ya que se podrían explotar los puntos vulnerables provocando daños gravísimos. Como internet no tiene fronteras, la vulneración de la seguridad en un Estado miembro podría tener repercusiones en muchos otros.

A fin de hacer frente a las posibles implicaciones graves en materia de seguridad para las infraestructuras digitales críticas, es necesario un enfoque común de la UE en relación con la seguridad de las redes 5G. Tras el Consejo Europeo de los días 21 y 22 de marzo de 2019, la Comisión formulará, como primer paso, una recomendación relativa a un planteamiento común de la UE en relación con los riesgos para la seguridad de las redes 5G, sobre la base de una evaluación coordinada de los riesgos en la UE y las correspondientes medidas de gestión, un marco eficaz de cooperación e intercambio de información y una conciencia compartida de la situación en la UE referida en particular a las redes de comunicación críticas. El debate sobre las posibles medidas debe abarcar el despliegue de tecnologías cuánticas para garantizar la seguridad de las redes y la protección de los datos almacenados[74].

El 12 de marzo de 2019, el Parlamento Europeo adoptó una Resolución sobre las amenazas para la seguridad relacionadas con la creciente presencia tecnológica china en la UE y sobre las posibles actuaciones a escala de la UE para reducirlas.

4. Cuestiones externas

[74] Véase también la Comunicación sobre la Iniciativa Europea de Computación en la Nube: construir en Europa una economía competitiva de los datos y del conocimiento [COM (2016) 178 final de 19.4.2016].

Las negociaciones entre la UE y Canadá sobre la **revisión del Acuerdo de registro de nombres de los pasajeros** avanzan a buen ritmo. La próxima Cumbre UE-Canadá, que se celebrará en Montreal los días 11 y 12 de abril de 2019, podría brindar nuevo impulso a las negociaciones.

La Comisión está preparando con las autoridades de los Estados Unidos la próxima evaluación conjunta del **Acuerdo de registro de nombres de los pasajeros entre la UE y los EE. UU.**[75], en consonancia con las disposiciones del mismo. Ya se está trabajando en la quinta revisión conjunta del **Acuerdo entre la UE y los EE.UU. sobre el Programa de Seguimiento de la Financiación del Terrorismo**[76]. En ella se revisarán las salvaguardias, los controles y las disposiciones en materia de reciprocidad del Acuerdo y se valorará el Programa como herramienta antiterrorista tanto para la UE como para los Estados Unidos.

La actual evolución de la situación en Siria ha puesto de relieve el debate sobre los **combatientes terroristas extranjeros** actualmente presentes o detenidos en zonas de conflicto. La UE puede prestar apoyo a los Estados miembros cuando así lo soliciten, especialmente en lo que se refiere al intercambio de información y el apoyo a las investigaciones penales, en particular mediante iniciativas de cooperación con los socios internacionales y a través de Europol, así como sobre la base de la experiencia y las mejores prácticas en materia de rehabilitación y reinserción desarrolladas en el contexto de la Red para la Sensibilización frente a la Radicalización. La UE también puede proporcionar apoyo para el desarrollo de capacidades a los terceros países más afectados por el retorno de los combatientes terroristas extranjeros. La decisión de proceder o no a la repatriación de los combatientes terroristas extranjeros y sus familias de las zonas de conflicto corresponderá a los Estados miembros interesados.

La UE y Egipto copresidieron la reunión plenaria del grupo de trabajo de África Oriental del **Foro Mundial contra el Terrorismo**, celebrada en Nairobi el 20 de febrero de 2019, con numerosos participantes de los sectores judicial y policial de Somalia, Kenia, Sudán, Uganda, Yibuti, Somalia, Etiopía, Yemen y Tanzania.

V. CONCLUSIÓN

La UE ha avanzado considerablemente en la labor conjunta hacia una Unión de la Seguridad genuina y efectiva, en particular con la adopción de una serie de iniciativas legislativas prioritarias por el Parlamento Europeo y el Consejo en las últimas semanas y meses. Sin embargo, en la perspectiva de las elecciones al Parlamento Europeo de mayo de 2019, es necesario seguir trabajando para adoptar de manera urgente las medidas necesarias en materia de seguridad. En particular, la Comisión insta a los colegisladores a entablar negociaciones sobre las normas propuestas para la eliminación de los contenidos terroristas en línea tan pronto como el Parlamento Europeo haya aprobado su mandato de negociación, con vistas a alcanzar un acuerdo durante la actual legislatura del Parlamento Europeo. Por lo que respecta a la propuesta de reforzar la Guardia Europea de Fronteras y Costas, las negociaciones se encuentran ya en la fase de diálogo tripartito, lo que demuestra que todas las instituciones están comprometidas a adoptar esa propuesta antes de las elecciones al Parlamento Europeo. La Comisión también pide a los Estados miembros que apliquen todas las medidas acordadas en el marco de la Unión de la Seguridad para garantizar que tengan pleno efecto y permitan

[75] DO L 215 de 11.8.2012, p. 5.
[76] DO L 195 de 27.7.2010, p. 5.

garantizar la seguridad de todos los ciudadanos.

Además, habida cuenta de la brevedad del plazo disponible para garantizar la preparación de la Unión antes de que los votantes europeos acudan a las urnas en mayo de 2019, la Comisión insta a todos los agentes implicados a redoblar los esfuerzos destinados a aumentar la resiliencia electoral para contrarrestar la desinformación. Antes del Consejo Europeo de los días 21 y 22 de marzo de 2019, es necesario que los Estados miembros intensifiquen su labor de coordinación e intercambio de información para contrarrestar la desinformación y proteger las elecciones contra otras amenazas cibernéticas, haciendo pleno uso de las herramientas que brinda la UE a tal efecto. Al mismo tiempo, las plataformas en línea deben acelerar sus esfuerzos en todos los Estados miembros para contribuir a garantizar la integridad de las elecciones al Parlamento Europeo de mayo de 2019. La Comisión seguirá apoyando y fomentando esta labor en las próximas semanas y meses para proteger la integridad de esos comicios.