COMISIÓN
EUROPEA

Bruselas, 24.7.2020
COM(2020) 605 final

COMUNICACIÓN DE LA COMISIÓN AL PARLAMENTO EUROPEO, AL CONSEJO EUROPEO, AL CONSEJO, AL COMITÉ ECONÓMICO Y SOCIAL EUROPEO Y AL COMITÉ DE LAS REGIONES

sobre la Estrategia de la UE para una Unión de la Seguridad

I. Introducción

Las orientaciones políticas de la Comisión han dejado claro que hemos de hacer todo lo que esté en nuestra mano cuando se trata de proteger a nuestros ciudadanos. La seguridad no es solo el fundamento de la seguridad personal, sino que también protege los derechos fundamentales y sienta las bases para la confianza y el dinamismo en nuestra economía, nuestra sociedad y nuestra democracia. Los europeos se enfrentan actualmente a un panorama de seguridad en evolución constante en el que influyen las amenazas cambiantes y otros factores, como el cambio climático, las tendencias demográficas y la inestabilidad política más allá de nuestras fronteras. La globalización, la libre circulación y la transformación digital siguen aportando prosperidad, facilitando nuestras vidas e impulsando la innovación y el crecimiento. Pero estos beneficios llevan aparejados riesgos y costes inherentes. Pueden ser manipulados por el terrorismo, la delincuencia organizada, el tráfico de drogas y la trata de seres humanos, todos ellos amenazas directas para los ciudadanos y nuestro modo de vida europeo. Los ciberataques y la ciberdelincuencia siguen aumentando. Asimismo, las amenazas a la seguridad se vuelven cada vez más complejas: se sustentan en la capacidad para trabajar de manera transfronteriza y en la interconectividad; sacan provecho de la difuminación de los límites entre los mundos físico y el digital; explotan a los grupos vulnerables y aprovechan las divergencias sociales y económicas. Los ataques pueden producirse en cualquier momento y dejar poco o ningún rastro; tanto los actores estatales como los no estatales pueden recurrir a una variedad de amenazas híbridas[1]; y lo que sucede fuera de la UE puede tener una incidencia crítica en la seguridad dentro de la UE.

La crisis de la COVID-19 ha transformado también nuestras nociones sobre las amenazas para la seguridad y la protección y las políticas correspondientes. Ha puesto de relieve la necesidad de garantizar la seguridad tanto en el entorno físico como en el digital. Ha puesto de manifiesto la importancia de una autonomía estratégica abierta para nuestras cadenas de suministro en términos de productos, servicios, infraestructuras y tecnologías vitales. Ha reforzado la necesidad de implicar a todos los sectores y a todas las personas en un esfuerzo común para garantizar que, ya de entrada, la UE esté más preparada y sea más resiliente, y que disponga, cuando se haga sentir la necesidad, de mejores herramientas de respuesta.

No es posible proteger a los ciudadanos a través únicamente de la actuación individual de los Estados miembros. Aprovechar nuestros puntos fuertes para trabajar juntos nunca ha sido más esencial, y la UE nunca ha tenido más potencial para marcar la diferencia. Puede dar ejemplo mejorando su sistema general de gestión de crisis y trabajando tanto dentro como fuera de sus fronteras para contribuir a la estabilidad global. Si bien la responsabilidad principal en materia de seguridad corresponde a los Estados miembros, estos últimos años han hecho que se comprenda cada vez mejor que la seguridad de un Estado miembro es la seguridad de todos. La UE puede aportar una respuesta multidisciplinar e integrada, ayudando a los actores estatales de los Estados miembros con los instrumentos y la información que necesitan[2].

---

[1] Aunque las definiciones de las amenazas híbridas varían, su objetivo es captar la combinación de actividades coercitivas y subversivas y de métodos convencionales y no convencionales (es decir, diplomáticos, militares, económicos y tecnológicos) que pueden utilizar de forma coordinada los actores estatales o no estatales para alcanzar objetivos específicos (sin dejar de mantenerse por debajo del umbral de la guerra declarada formalmente). Véase JOIN(2016) 18 final.

[2] Por ejemplo, a través de los servicios prestados por el programa espacial de la UE, como Copernicus, que proporciona datos y aplicaciones de observación de la Tierra para la vigilancia de las fronteras, la seguridad

La UE también puede garantizar que la política de seguridad esté basada en nuestros valores comunes europeos —respetando y haciendo respetar el Estado de Derecho, la igualdad[3] y los derechos fundamentales y garantizando la transparencia, la rendición de cuentas y el control democrático— para que políticas cuenten con un fundamento adecuado de confianza. Puede construir una Unión de la Seguridad genuina y efectiva en la que los derechos y libertades de las personas estén bien protegidos. La seguridad y el respeto de los derechos fundamentales no son objetivos contradictorios, sino coherentes y complementarios. Nuestros valores y derechos fundamentales deben ser la base de las políticas de seguridad, garantizando los principios de necesidad, proporcionalidad y legalidad, y con las salvaguardias adecuadas para la rendición de cuentas y el acceso a la vía judicial, permitiendo al mismo tiempo una respuesta eficaz para proteger a las personas, en particular a los más vulnerables.

Existen ya instrumentos jurídicos, prácticos y de apoyo importantes, pero estos deben reforzarse y emplearse mejor. Se ha avanzado mucho a la hora de mejorar el intercambio de información y la cooperación de los servicios de inteligencia con los Estados miembros, así como de reducir el perímetro de actuación de terroristas y delincuentes. Pero persiste la fragmentación.

El trabajo también debe ir más allá de las fronteras de la UE. Proteger a la Unión y a sus ciudadanos ya no consiste tan solo en garantizar la seguridad dentro de las fronteras de la UE, sino también a abordar la dimensión exterior de la seguridad. El enfoque de la UE en materia de seguridad exterior en el marco de la Política Exterior y de Seguridad Común (PESC) y de la Política Común de Seguridad y Defensa (PCSD) seguirá siendo un componente esencial de los esfuerzos de la UE por mejorar la seguridad en la UE. La cooperación con terceros países y a nivel mundial para hacer frente a los retos comunes es fundamental para una respuesta eficaz y global; asimismo, la estabilidad y la seguridad en la vecindad de la UE es fundamental para la propia seguridad de la UE.

Basándose en los trabajos realizados anteriormente por el Parlamento Europeo[4], el Consejo[5] y la Comisión[6], esta nueva estrategia muestra que una Unión de la Seguridad genuina y eficaz debe combinar un núcleo sólido de instrumentos y políticas para garantizar la seguridad en la práctica con el reconocimiento de que la seguridad tiene implicaciones para todos los segmentos de la sociedad y para todas las políticas públicas. La UE debe garantizar un entorno seguro para todos, independientemente de su origen racial o étnico, de su religión o creencias, o de su género, edad u orientación sexual.

Esta Estrategia abarca el período 2020-2025 y se centra en la creación de las capacidades y los medios para garantizar un entorno de seguridad con garantías de futuro. Establece un enfoque en materia de seguridad que incluye a la sociedad en su conjunto y que puede responder eficazmente a un panorama de amenazas en rápida transformación de forma

---

marítima, la aplicación de la ley, la lucha contra la piratería, la disuasión del tráfico ilícito de drogas y la gestión de emergencias.

[3] Una Unión de la igualdad: Estrategia para la Igualdad de Género 2020-2025, COM(2020) 152.

[4] Por ejemplo, la labor de la Comisión TERR del Parlamento Europeo, que informó en noviembre de 2018.

[5] De las Conclusiones del Consejo de junio de 2015 sobre una «Estrategia Renovada de Seguridad Interior» a los más recientes resultados de las sesiones del Consejo de diciembre de 2019.

[6] Aplicación de la Agenda Europea de Seguridad para luchar contra el terrorismo y allanar el camino hacia una Unión de la Seguridad genuina y efectiva [COM(2016) 230 final, de 20.4.2016]. Véase la reciente evaluación de la aplicación de la legislación en el ámbito de la seguridad interior: Aplicación de la legislación en materia de Justicia y Asuntos de Interior en el ámbito de la seguridad interior: 2017-2020 [SWD(2020) 135].

coordinada. Define las prioridades estratégicas y las acciones correspondientes para hacer frente a los riesgos digitales y físicos de manera integrada en todo el ecosistema de la Unión de la Seguridad, centrándose en los ámbitos en los que la UE puede aportar más valor. Su objetivo es ofrecer un dividendo de seguridad para proteger a todos en la UE.

II. Un panorama europeo de amenazas para la seguridad en rápida transformación

Para la seguridad, la prosperidad y el bienestar de los ciudadanos es necesario que estos estén bien protegidos. Las amenazas para dicha seguridad dependen del grado en que sus vidas y sus medios de subsistencia sean vulnerables. Cuanto mayor sea la vulnerabilidad, mayor será el riesgo de que esta sea aprovechada. Tanto las vulnerabilidades como las amenazas se encuentran en un estado de transformación constante, y la UE necesita adaptarse.

Nuestra vida cotidiana depende de una gran variedad de servicios, como la energía, el transporte, las finanzas y los servicios sanitarios. Estos dependen, a su vez, de una infraestructura tanto física como digital, lo cual incrementa la vulnerabilidad y el potencial de perturbaciones. Durante la pandemia de COVID-19, las nuevas tecnologías han permitido seguir funcionando a numerosas empresas y servicios públicos, al mantenernos conectados a través del teletrabajo o preservar la logística de las cadenas de suministro. Pero también ha abierto la puerta a un extraordinario aumento de los ataques malintencionados, que intentan sacar partido a las perturbaciones causadas por la pandemia y a la transición al trabajo digital en el hogar con fines delictivos[7]. La escasez de bienes ha creado nuevas oportunidades para la delincuencia organizada. Las consecuencias podrían haber sido fatales si hubiesen perturbado los servicios sanitarios esenciales en el momento de mayor presión.

Las formas cada vez más numerosas en que las tecnologías digitales nos benefician en nuestras vidas también han convertido la **ciberseguridad** de las tecnologías en una cuestión de importancia estratégica[8]. Los hogares, los bancos, los servicios financieros y las empresas (en particular las pymes) se ven gravemente afectados por los ciberataques. El perjuicio potencial se multiplica aún más por la interdependencia de los sistemas físicos y digitales; cualquier impacto físico afectará también a los sistemas digitales, mientras que los ciberataques contra sistemas de información e infraestructuras digitales pueden interrumpir el funcionamiento de los servicios esenciales[9]. El auge del internet de las cosas y el uso creciente de la inteligencia artificial aportarán nuevos beneficios, pero también un nuevo conjunto de riesgos.

Nuestro mundo depende de infraestructuras digitales y tecnologías y sistemas en línea que nos permiten crear empresas, consumir productos y disfrutar de servicios. Todos se basan en

---

[7] Europol: Beyond the pandemic. How COVID-19 will shape the serious and organised crime landscape in the EU, abril de 2020 (Más allá de la pandemia: Así modificará la COVID-19 el panorama de la delincuencia grave y organizada en la UE).

[8] Recomendación de la Comisión sobre la ciberseguridad de las redes 5G [C(2019) 2335]; Comunicación de la Comisión sobre el despliegue seguro de las redes 5G en la UE [COM(2020) 50].

[9] En marzo de 2020, el Hospital universitario de Brno en Chequia sufrió un ciberataque que lo obligó a redirigir a los pacientes y a posponer operaciones (Europol: Pandemic profiteering. How criminals exploit the COVID-19 crisis) (Beneficiándose de la pandemia: cómo los delincuentes explotan la crisis de la COVID-19). La inteligencia artificial puede utilizarse indebidamente para realizar ataques digitales, políticos y físicos, así como para la vigilancia. La recogida de datos mediante el internet de las cosas puede utilizarse para vigilar a las personas (relojes inteligentes, asistentes virtuales, etc.).

la comunicación y la interacción. La dependencia del mundo en línea ha abierto la puerta a una ola de **ciberdelincuencia**[10]. La «ciberdelincuencia entendida como servicio» y la economía subterránea ciberdelictiva ofrecen un fácil acceso a los productos y servicios de la ciberdelincuencia. Los delincuentes se adaptan rápidamente al uso de las nuevas tecnologías para sus propios fines. Por ejemplo, los medicamentos falsos o adulterados se han infiltrado en la cadena de suministro legítima de productos farmacéuticos[11]. El crecimiento exponencial del material de abuso sexual de menores en línea[12] ha puesto de manifiesto las consecuencias sociales de la evolución de las pautas delictivas. Una encuesta reciente ha mostrado que a la mayoría de los ciudadanos de la UE (el 55 %) le preocupa que los delincuentes y los defraudadores puedan acceder a sus datos[13].

El **entorno mundial** intensifica también estas amenazas. La asertividad de las políticas industriales de terceros países, junto con el robo continuo de propiedad intelectual posibilitado por los medios cibernéticos, están cambiando el paradigma estratégico de protección y promoción de los intereses europeos. Esta situación se ve agravada por el aumento de las aplicaciones que pueden tener doble uso, que hacen que un sector de tecnología civil fuerte constituya un importante activo para las capacidades de defensa y seguridad. El espionaje industrial tiene una incidencia significativa en la economía, el empleo y el crecimiento de la UE: se estima que el robo cibernético de secretos comerciales cuesta a la UE 60 000 millones EUR[14]. Esto requiere una profunda reflexión sobre la manera en que las dependencias y el aumento de la exposición a las ciberamenazas afectan a la capacidad de la UE para proteger tanto a las personas como a las empresas.

La crisis de la COVID-19 también ha puesto de relieve la forma en que las divisiones sociales y la incertidumbre crean una vulnerabilidad en materia de seguridad. Esto aumenta las posibilidades de que se produzcan ataques **híbridos** y más sofisticados por parte de actores estatales y no estatales y de que se aprovechen las vulnerabilidades a través de una combinación de ciberataques, daños a infraestructuras críticas[15], campañas de desinformación y la radicalización del discurso político.[16]

Al mismo tiempo, las amenazas más tradicionales siguen evolucionando. En 2019 se dio una tendencia a la baja de los **atentados terroristas** en la UE. Sin embargo, el riesgo para los ciudadanos de la UE de ataques yihadistas perpetrados o inspirados por Daesh y Al Qaeda y

---

[10] Según algunas previsiones, el coste de las violaciones de la seguridad de datos alcanzará los 5 billones de dólares al año de aquí a 2024, frente a los 3 billones de dólares en 2015 (*Juniper Research, The Future of Cybercrime & Security* [El Futuro de la Ciberdelincuencia y de la Seguridad]).

[11] Un estudio de 2016 (Legiscript) estimó que, a nivel mundial, solo el 4 % de las farmacias de internet operan legalmente, y que los principales objetivos de las 30 000 a 35 000 farmacias en línea ilegales que operan en línea son los consumidores de la UE.

[12] Estrategia de la UE para una lucha más eficaz contra el abuso sexual de menores, COM(2020) 607.

[13] Agencia de los Derechos Fundamentales de la Unión Europea (2020), *Your rights matter: Security concerns and experiences* (Tus derechos importan: preocupaciones y experiencias en materia de seguridad), encuesta sobre los derechos fundamentales, Oficina de Publicaciones, Luxemburgo.

[14] The scale and impact of industrial espionage and theft of trade secrets through cyber (La escala y la incidencia del espionaje industrial y el robo de secretos comerciales por medios cibernéticos), 2018.

[15] Las infraestructuras críticas son esenciales para las funciones vitales de la sociedad, la salud, la seguridad, la protección y el bienestar económico o social, cuya perturbación o destrucción tiene una incidencia significativa (Directiva 2008/114/CE del Consejo).

[16] El 97 % de los ciudadanos de la UE se han visto confrontados a noticias falsas, el 38 % de forma diaria. Véase JOIN(2020) 8 final.

sus filiales sigue siendo alto[17]. Paralelamente, también está aumentando la amenaza de violencia de la extrema derecha[18]. Los atentados inspirados por el racismo deben suscitar una gran preocupación: los atentados terroristas antisemitas mortales perpetrados en Halle recuerdan la necesidad de intensificar la respuesta con arreglo a la Declaración del Consejo de 2018[19]. A una de cada cinco personas en la UE le preocupa la posibilidad de un atentado terrorista en los próximos 12 meses[20]. La gran mayoría de los recientes atentados terroristas fueron ataques «de nivel tecnológico bajo», individuos solitarios que atacan a otros individuos en espacios públicos, mientras que la propaganda terrorista en línea cobró una importancia inédita con la retransmisión en directo de los atentados de Christchurch[21]. La amenaza que suponen los individuos radicalizados sigue siendo elevada y podría intensificarse por el retorno de combatientes terroristas extranjeros y por los extremistas liberados de la prisión[22].

La crisis también ha puesto de manifiesto la manera en que las amenazas existentes pueden evolucionar si se dan nuevas circunstancias. Los grupos de **delincuencia organizada** han aprovechado la escasez de bienes como ocasión para crear nuevos mercados ilícitos. El tráfico de drogas ilícitas sigue siendo el mayor mercado delictivo de la UE, con un valor estimado mínimo del mercado minorista de 30 000 millones EUR al año en la UE[23]. La trata de seres humanos persiste: las estimaciones arrojan un beneficio global anual para todas las formas de explotación de casi 30 000 millones EUR[24]. El volumen del comercio internacional de productos farmacéuticos falsificados alcanzó los 38 900 millones EUR[25]. Al mismo tiempo, los bajos índices de decomiso permiten a los delincuentes seguir ampliando sus actividades delictivas e infiltrándose en la economía legal[26]. A los delincuentes y los terroristas les resulta más fácil acceder a las armas de fuego desde el mercado en línea y a través de nuevas tecnologías como la impresión tridimensional[27]. El uso de la inteligencia artificial, las nuevas tecnologías y la robótica seguirá aumentando el riesgo de que los delincuentes aprovechen las ventajas de la innovación con fines malintencionados[28].

---

17 Trece Estados miembros de la UE notificaron un total de 119 atentados terroristas completados, fallidos y frustrados, con diez muertos y veintisiete heridos (Europol, *European Union Terrorism Situation and Trend Report*, 2020).

18 En 2019 se produjeron seis atentados terroristas de tendencia derechista (uno llegó a completarse, uno fracasó y cuatro fueron frustrados: tres Estados miembros), frente a un único atentado en 2018; asimismo, se produjeron muertes adicionales en sucesos no calificados de terrorismo (Europol, 2020).

19 Véase también la Declaración del Consejo sobre la lucha contra el antisemitismo y el desarrollo de un planteamiento de seguridad común para proteger mejor a las comunidades e instituciones judías en Europa.

20 Agencia de los Derechos Fundamentales de la Unión Europea: *Your rights matter: Security concerns and experiences* (Tus derechos importan: preocupaciones y experiencias en materia de seguridad), 2020.

21 Entre julio de 2015 y el final de 2019, Europol encontró contenidos terroristas en 361 plataformas (Europol, 2020).

22 Europol: *A Review of Transatlantic Best Practices for Countering Radicalisation in Prisons and Terrorist Recidivism* (Examen de las mejores prácticas transatlánticas para luchar contra la radicalización en las cárceles y contra la reincidencia terrorista), 2019.

23 «Informe Europeo sobre el mercado de las drogas» de 2019 del EMCDDA y Europol.

24 Informe de Europol sobre la trata de seres humanos, Modelo de Negocio Financiero (2015).

25 Informe de la EUIPO y la OCDE sobre El comercio de productos farmacéuticos falsificados

26 Informe sobre «Recuperación de activos y decomiso: Garantizar que el delito no resulte provechoso» [COM(2020) 217].

27 En 2017, se utilizaron armas de fuego en el 41 % de todos los atentados terroristas (Europol, 2018).

28 En julio de 2020, las autoridades judiciales y policiales de Francia y los Países Bajos, junto con Europol y Eurojust, presentaron la investigación conjunta del desmantelamiento de EncroChat, una red telefónica cifrada utilizada por redes delictivas implicadas en ataques violentos, corrupción, intentos de asesinato y transportes de droga a gran escala.

Estas amenazas pueden abarcar varias categorías de forma transversal y afectar a diferentes partes de la sociedad de modos distintos. Todas ellas suponen importantes amenazas para particulares y empresas y exigen una respuesta global y coherente a nivel de la UE. Cuando las vulnerabilidades de seguridad pueden proceder incluso de pequeños objetos domésticos interconectados como un frigorífico o una máquina de café conectados a internet, ya no es posible encomendarse únicamente a los actores estatales tradicionales para que velen por nuestra seguridad. Los operadores económicos deben asumir una mayor responsabilidad respecto de la ciberseguridad de los productos y servicios que comercializan; al mismo tiempo, los individuos también han de tener, por lo menos, nociones básicas de ciberseguridad para estar en condiciones de protegerse.

III. Una respuesta coordinada de la UE para el conjunto de la sociedad

La UE ya ha demostrado cómo puede aportar valor añadido real. Desde 2015, la Unión de la Seguridad ha introducido nuevos vínculos en la forma de plantear las políticas de seguridad a nivel de la UE. Pero es necesario hacer más para involucrar al conjunto de la sociedad, incluidos los gobiernos a todos los niveles, las empresas de todos los sectores y los particulares de todos los Estados miembros. La sensibilización cada vez mayor sobre los riesgos de la dependencia[29] y sobre la necesidad de una estrategia industrial europea sólida[30] apuntan a una UE con una masa crítica industrial, producción tecnológica y una cadena de suministro resiliente. Para ser fuertes también es necesario respetar plenamente los derechos fundamentales y de los valores de la UE, que son un requisito previo para unas políticas de seguridad legítimas, eficaces y sostenibles. La estrategia de la Unión de la Seguridad establece líneas de trabajo concretas que se han de impulsar. Se estructura en torno a los siguientes objetivos comunes:

- ***Desarrollar capacidades y medios para la detección temprana, la prevención y la respuesta rápida a las crisis:*** Europa necesita ser más resiliente para prevenir y protegerse frente a crisis futuras y resistir. Necesitamos desarrollar capacidades y medios para la detección temprana y la respuesta rápida a las crisis de seguridad mediante un enfoque integrado y coordinado, tanto de forma global como mediante iniciativas sectoriales (como las relativas a los sectores financiero, energético, judicial, policial, sanitario, marítimo y del transporte) y aprovechar los instrumentos e iniciativas existentes[31]. La Comisión también presentará propuestas para un sistema de gestión de crisis amplio dentro de la UE, que también podría ser pertinente en materia de seguridad.
- ***Centrarse en los resultados***: Una estrategia basada en el rendimiento debe fundamentarse en una atenta evaluación de las amenazas y los riesgos para orientar nuestros esfuerzos de la mejor manera posible. Requiere la definición y la aplicación de las normas apropiadas y los instrumentos adecuados. Requiere información estratégica

[29] Los riesgos de la dependencia extranjera implican una mayor exposición a posibles amenazas, desde el aprovechamiento de las vulnerabilidades de las infraestructuras informáticas con potencial para comprometer infraestructuras críticas (por ejemplo, energéticas, de transporte, bancarias o sanitarias) o la toma del control de los sistemas de control industriales, a una mayor capacidad para el robo de datos o el espionaje.

[30] Comunicación de la Comisión «Una nueva estrategia industrial para Europa», COM(2020) 102.

[31] Como el Dispositivo de la UE de Respuesta Política Integrada a las Crisis (RPIC), el Centro de Coordinación de la Respuesta a Emergencias, la Recomendación de la Comisión sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala [C(2017) 6100] y el protocolo de actuación conjunta de la UE para contrarrestar las amenazas híbridas [SWD(2016) 227].

fiable como fundamento de las políticas de seguridad de la UE. Cuando sea necesaria legislación de la UE, esta deberá ser objeto de seguimiento para velar por su íntegra aplicación, a fin de evitar la fragmentación y el surgimiento de lagunas susceptibles de aprovechamiento. La aplicación efectiva de esta Estrategia dependerá también de que se consigan fondos suficientes en el próximo período de programación 2021-2027, también para las agencias de la UE correspondientes.

- ***Conectar a todos los actores de los sectores público y privado en un esfuerzo común:*** Actores clave de los sectores tanto público como privado se han mostrado reacios a compartir la información pertinente en materia de seguridad, ya fuese por temor a comprometer la seguridad nacional o por motivos de competitividad.[32] Pero nunca somos más eficaces que cuando nos organizamos todos para apoyarnos mutuamente. Esto significa, en primer lugar, una cooperación más intensa entre los Estados miembros en la que participen las autoridades policiales, judiciales y otros poderes públicos, y con las instituciones y agencias de la UE, a fin de lograr un mejor entendimiento y de intercambiar la información necesaria para alcanzar soluciones comunes. La cooperación con el sector privado es también clave, tanto más cuanto que la industria posee una parte considerable de la infraestructura digital y no digital esencial para luchar contra la delincuencia y el terrorismo de forma efectiva. Los propios particulares pueden también contribuir, por ejemplo a través del desarrollo de las competencias y de la sensibilización para combatir la ciberdelincuencia y la desinformación. Por último, este esfuerzo común debe extenderse más allá de nuestras fronteras mediante la creación de vínculos más estrechos con socios afines.

IV. Proteger a todos en la UE: prioridades estratégicas para la Unión de la Seguridad

La UE goza de una situación privilegiada para responder a estas nuevas amenazas y retos mundiales. El análisis de las amenazas mencionado indica que existen cuatro prioridades estratégicas interdependientes en las que es necesario trabajar a nivel de la UE, respetando plenamente los derechos fundamentales: i) un entorno de seguridad con garantías de futuro; ii) hacer frente a las amenazas cambiantes; iii) proteger a los europeos del terrorismo y la delincuencia organizada; y iv) un ecosistema europeo de seguridad sólido.

1. Un entorno de seguridad con garantías de futuro

Protección y resiliencia de las infraestructuras críticas

Los individuos dependen de las infraestructuras clave en su vida cotidiana para viajar, trabajar, beneficiarse de servicios públicos esenciales —como la atención hospitalaria, el transporte, o el suministro de energía— o para ejercer sus derechos democráticos. Si estas infraestructuras no tienen la protección y la resiliencia necesarias, los atentados pueden provocar graves perturbaciones —físicas o digitales— tanto en Estados miembros concretos como, potencialmente, en toda la UE.

El actual marco de la UE para la protección y la resiliencia de las infraestructuras críticas[33] no ha conseguido seguir el ritmo de la evolución de los riesgos. La creciente

[32] Comunicación conjunta «Resiliencia, disuasión y defensa: Reforzar la ciberseguridad de la UE» [JOIN(2017) 450].

[33] Directiva 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (DO L 194 de 19.7.2016); Directiva 2008/114/CE del

interdependencia significa que las perturbaciones en un sector pueden tener un impacto inmediato en las operaciones de otros sectores: un atentado contra la producción de electricidad podría paralizar las telecomunicaciones, los hospitales, los bancos o los aeropuertos, mientras que un ataque contra la infraestructura digital podría dar lugar a perturbaciones en las redes eléctricas o financieras. A medida que nuestra economía y nuestra sociedad migran cada vez más al ámbito digital, los riesgos de este tipo se van agravando. El marco legislativo debe tener en cuenta esta mayor interconexión e interdependencia con unas medidas contundentes de protección de las infraestructuras y de resiliencia, tanto cibernéticas como físicas. Los servicios esenciales, incluidos aquellos que se basan en las infraestructuras espaciales, han de protegerse adecuadamente contra las amenazas actuales y previstas, pero también ser resilientes. Esto implica la capacidad de un sistema de prepararse y realizar planes de cara a los acontecimientos adversos, así como para encajar sus consecuencias, recuperarse y adaptarse más eficazmente a ellos.

Al mismo tiempo, los Estados miembros han hecho uso de su margen de apreciación aplicando de maneras distintas la legislación vigente. La fragmentación resultante puede socavar el mercado interior y hacer más difícil la coordinación transfronteriza, sobre todo, obviamente, en las regiones fronterizas. Los operadores que prestan servicios esenciales en diferentes Estados miembros deben observar distintos regímenes de notificación. La Comisión está estudiando si el establecimiento de **nuevos marcos para las infraestructuras tanto físicas como digitales** podrían aportar mayor coherencia y un enfoque más coherente para garantizar la prestación fiable de servicios esenciales. Este marco debe ir acompañado de **iniciativas sectoriales** específicas para hacer frente a los riesgos específicos a que se enfrentan las infraestructuras críticas, como, por ejemplo, las de transporte, las espaciales, las energéticas, las financieras y las sanitarias[34]. Dada la gran dependencia del sector financiero de los servicios informáticos y su gran vulnerabilidad frente a los ciberataques, una primera medida consistirá en una iniciativa sobre la resiliencia operativa digital para los sectores financieros. Debido a las sensibilidades particulares y al impacto del sistema energético, una iniciativa específica impulsará una mayor resiliencia de las infraestructuras energéticas críticas frente a las amenazas físicas, cibernéticas e híbridas, garantizando unas condiciones de competencia equitativas para los operadores energéticos a través de las fronteras.

Los efectos con repercusiones en materia de seguridad de las inversiones extranjeras directas que puedan afectar a infraestructuras críticas o a tecnologías críticas se someterán también a las evaluaciones llevadas a cabo por los Estados miembros de la UE y la Comisión en el nuevo marco europeo de supervisión de la inversión extranjera directa[35].

La UE también puede crear nuevos instrumentos para incrementar la resiliencia de las infraestructuras críticas. El internet mundial ha mostrado hasta ahora un alto nivel de

---

Consejo, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.

[34] Dado que el sector sanitario ha estado sometido a tensiones, sobre todo durante la crisis de la COVID-19, la Comisión también estudiará iniciativas para reforzar el marco de seguridad sanitaria de la UE y las agencias competentes de la UE para responder a las amenazas transfronterizas graves para la salud.

[35] Con su plena entrada en vigor el 11 de octubre de 2020, el Reglamento (UE) 2019/452 del Parlamento Europeo y del Consejo, de 19 de marzo de 2019, por el que se establece un marco para el control de las inversiones extranjeras directas en la Unión, dotará a la UE de un nuevo mecanismo de cooperación en materia de inversiones directas desde fuera de la UE que puedan afectar a la seguridad o al orden público. De conformidad con este Reglamento, los Estados miembros y la Comisión evaluarán los riesgos potenciales vinculados a dicha inversión extranjera directa y, cuando sea apropiado y pertinente para más de un Estado miembro, propondrán medidas adecuadas para mitigar esos riesgos.

resiliencia, en particular por lo que se refiere a la capacidad de soportar el aumento de los volúmenes de tráfico. No obstante, debemos estar preparados para posibles crisis futuras que supongan una amenaza para la seguridad, la estabilidad y la resiliencia de internet. Velar por que internet siga funcionando a pleno rendimiento implica una prevención enérgica contra los ciberincidentes y las actividades malintencionadas en línea, así como limitar la dependencia de las infraestructuras y los servicios ubicados fuera de Europa. Para ello será necesario combinar legislación, con la revisión de las normas vigentes para garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la UE; una mayor inversión en investigación e innovación; y estudiar de la posibilidad de emplear o reforzar infraestructuras y recursos básicos, especialmente el sistema de nombres de dominio[36].

Un elemento clave para proteger los activos digitales esenciales de la UE y nacionales consiste en ofrecer a las infraestructuras críticas a un canal de comunicaciones seguras. La Comisión está trabajando con los Estados miembros para crear una infraestructura cuántica de seguridad certificada de extremo a extremo, terrestre y espacial, en combinación con el sistema gubernamental de comunicaciones por satélite seguro establecido en el Reglamento sobre el Programa Espacial[37].

Ciberseguridad

El número de ciberataques continúa aumentando[38]. Estos ataques son más sofisticados que nunca, proceden de una amplia gama de fuentes dentro y fuera de la UE, y están dirigidos a los ámbitos de máxima vulnerabilidad. A menudo se trata de agentes estatales o respaldados por un Estado que atacan infraestructuras digitales clave como los principales proveedores de servicios en nube[39]. Se ha puesto de manifiesto que los riesgos de ciberseguridad suponen también una amenaza importante para el sistema financiero. El Fondo Monetario Internacional ha estimado que las pérdidas anuales debidas a ciberataques ascienden a un 9 % de los ingresos netos de los bancos en todo el mundo, es decir, alrededor de 100 000 millones de dólares[40]. La transición a los dispositivos conectados reportará grandes beneficios para los usuarios: sin embargo, al haber menos datos almacenados y tratados en los centros de datos, y más tratados de una forma más cercana al usuario «en el borde[41]», la ciberseguridad ya no podrá centrarse en la protección de nodos centrales[42].

En 2017, la UE presentó un enfoque en materia de ciberseguridad centrado en el fortalecimiento de la resiliencia, una respuesta rápida y una disuasión efectiva[43]. La UE debe

---

[36] Un sistema de nombres de dominio (DNS) es un sistema de asignación de nombres jerárquico y descentralizado para ordenadores, servicios y otros recursos conectados a internet o a una red privada. «Traduce» los nombres de dominio a las direcciones IP necesarias para localizar e identificar servicios y dispositivos informáticos.

[37] Propuesta de Reglamento por el que se crean el Programa Espacial de la Unión y la Agencia de la Unión Europea para el Programa Espacial. COM(2018) 447.

[38] https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

[39] Los ataques distribuidos de denegación de servicios siguen siendo una amenaza permanente: los principales proveedores han tenido que contrarrestar ataques masivos de este tipo, como el dirigido contra Amazon Web Services en febrero de 2020.

[40] https://blogs.imf.org/2018/06/22/estimating-cyber-risk-for-the-financial-sector/.

[41] La computación en el borde es una arquitectura informática abierta y distribuida con capacidad informática descentralizada y que hace posible el funcionamiento de la informática móvil y de las tecnologías del internet de los de las cosas (IdC). En la computación en el borde, los datos son tratados por el propio dispositivo o por un ordenador o servidor local, en lugar de ser transmitidos a un centro de datos.

[42] Comunicación titulada «Una Estrategia Europea de Datos», COM(2020) 66 final.

[43] Comunicación conjunta «Resiliencia, disuasión y defensa: Reforzar la ciberseguridad de la UE» [JOIN(2017) 450].

ahora asegurarse de que sus capacidades en materia de ciberseguridad sigan el ritmo de la realidad a fin de aportar resiliencia y una respuesta adecuada. Esto requiere un planteamiento que tenga verdaderamente en cuenta a la sociedad en su conjunto, y que las instituciones, órganos y organismos de la UE, los Estados miembros, la industria, el mundo académico y las personas otorguen a la ciberseguridad la prioridad necesaria[44]. Este enfoque horizontal debe complementarse a su vez con enfoques sectoriales en materia de ciberseguridad para ámbitos como la energía, los servicios financieros, el transporte o la sanidad. La próxima fase del trabajo de la UE debe llevarse a cabo de forma conjunta en una Estrategia de Ciberseguridad Europea revisada.

El estudio de formas nuevas y reforzadas de cooperación entre los servicios de inteligencia, el INTCEN, y otras organizaciones implicadas en cuestiones de seguridad debe formar parte de los esfuerzos para fortalecer la ciberseguridad y combatir el terrorismo, el extremismo, el radicalismo y las amenazas híbridas.

Habida cuenta de la instalación en curso de la **infraestructura para las redes 5G** en toda la UE y de la posible dependencia de muchos servicios críticos de dichas redes, las consecuencias de una perturbación sistémica y generalizada serían especialmente graves. El proceso establecido por la Recomendación de la Comisión de 2019 sobre la ciberseguridad de las redes 5G[45] ha dado lugar a una actuación específica de los Estados miembros respecto de las medidas clave establecidas en el «conjunto de instrumentos» para las redes 5G[46].

Una de las necesidades más importantes a largo plazo es desarrollar una cultura de la **ciberseguridad a través del diseño**, de moda que los productos y servicios sean seguros desde el principio. Una importante contribución a este fin será el nuevo marco de certificación de la ciberseguridad en virtud del Reglamento sobre la Ciberseguridad[47]. La elaboración de este marco ya ha comenzado, con dos sistemas de certificación que se encuentran ya en fase de preparación y la definición de prioridades para otros regímenes prevista para finales de este año. La cooperación entre la Agencia de la Unión Europea para la Ciberseguridad (ENISA), las autoridades de protección de datos y el Comité Europeo de Protección de Datos[48] reviste una importancia fundamental en este ámbito.

La Comisión ha detectado ya la necesidad de que una **unidad informática conjunta** se ocupe de que exista una cooperación operativa estructurada y coordinada. Esto podría incluir un mecanismo de asistencia mutua en tiempos de crisis a nivel de la UE. Sobre la base de la aplicación de la recomendación de Plan Director[49], la unidad informática conjunta podría generar confianza entre los distintos actores del ecosistema europeo de ciberseguridad y ofrecer un servicio clave a los Estados miembros. La Comisión iniciará conversaciones con

---

[44] El informe «Cybersecurity – our digital Anchor» (Ciberseguridad: nuestro pilar digital), del Centro Común de Investigación, ofrece una perspectiva multidimensional del crecimiento de la ciberseguridad durante los últimos cuarenta años.

[45] Recomendación de la Comisión sobre la ciberseguridad de las redes 5G [COM(2019) 2335 final]. La Recomendación prevé su propia revisión en el último trimestre de 2020.

[46] Véase el Informe del Grupo de Cooperación SRI sobre la utilización del conjunto de instrumentos, de 24 de julio de 2020.

[47] Reglamento 2019/881 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación (Reglamento sobre la Ciberseguridad).

[48] Comunicación sobre la protección de datos como pilar del empoderamiento de los ciudadanos y del enfoque de la UE para la transición digital: dos años de aplicación del Reglamento General de Protección de Datos [COM(2020) 264].

[49] Recomendación 2017/1584 de la Comisión sobre la respuesta coordinada a los incidentes y crisis de ciberseguridad a gran escala

las partes interesadas pertinentes (empezando por los Estados miembros) y establecerá un proceso, unos objetivos intermedios y un calendario claros para finales de 2020.

También son importantes las normas comunes en materia de seguridad de la información y ciberseguridad para todas las instituciones, órganos y organismos de la UE. El objetivo debe ser crear unas normas comunes vinculantes y exigentes para el intercambio seguro de información y la seguridad de las infraestructuras y los sistemas digitales en todas las instituciones, órganos y organismos de la UE. Este nuevo marco debe servir de fundamento a una cooperación operativa sólida y eficiente en materia de ciberseguridad en las instituciones, órganos y organismos de la UE, centrada en el papel del Equipo de respuesta a emergencias informáticas (CERT-UE) para las instituciones, órganos y organismos de la UE.

Dada su naturaleza global, la creación y el mantenimiento de **asociaciones internacionales** sólidas es fundamental para seguir previniendo, desincentivando y respondiendo a los ciberataques. El marco para una respuesta diplomática conjunta de la UE a las actividades informáticas malintencionadas (conjunto de instrumentos de ciberdiplomacia)[50] establece medidas en el marco de la política exterior y de seguridad común, incluyendo medidas restrictivas (sanciones), que pueden utilizarse contra las actividades perjudiciales para sus intereses políticos, económicos y de seguridad. La UE también debe profundizar su trabajo a través de fondos de desarrollo y cooperación para facilitar la creación de capacidades a fin de apoyar a los Estados socios en el fortalecimiento de sus ecosistemas digitales, la adopción de reformas legislativas nacionales y la adaptación a las normas internacionales. Esto aumenta la resiliencia de la comunidad en general y su capacidad para contrarrestar y responder eficazmente a las amenazas cibernéticas. Esto incluye trabajos específicos para promover las normas de la UE y la legislación pertinente para incrementar la ciberseguridad de los países socios en la vecindad[51].

Protección de los espacios públicos

Los recientes atentados terroristas se han dirigido contra **espacios públicos**, incluidos los lugares de culto y los centros de transporte, aprovechando su carácter abierto y accesible. El aumento del terrorismo provocado por el extremismo motivado política o ideológicamente ha agravado aún más esta amenaza. Esto requiere tanto una mayor protección física de dichos lugares como unos sistemas de detección adecuados, sin socavar las libertades de los ciudadanos[52]. La Comisión mejorará la cooperación entre los sectores público y privado para la protección de los espacios públicos con financiación, intercambios de experiencias y buenas prácticas, orientaciones específicas[53] y recomendaciones[54]. También formarán parte del enfoque las campañas de sensibilización, los requisitos de rendimiento, las pruebas de los equipos de detección y la mejora de los controles de antecedentes para hacer frente a las

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

[51] Véanse las directrices para el desarrollo de la capacidad cibernética exterior de la UE adoptadas en las conclusiones del Consejo de 26 de junio de 2018.

[52] Los sistemas de identificación biométrica a distancia merecen ser objeto de un examen específico. Los puntos de vista iniciales de la Comisión se exponen en el Libro Blanco de la Comisión, de 19 de febrero de 2020, sobre la inteligencia artificial [COM (2020) 65].

[53] Por ejemplo, la *Guidance on selecting proper security barrier solutions for public space protection* (Guía para seleccionar las soluciones adecuadas de barreras de seguridad para la protección de los espacios públicos) (https://publications.jrc.ec.europa.eu/repository/bitstream/JRC120307/hvm_v3.pdf).

[54] En el Documento de trabajo de los servicios de la Comisión SWD (2019) 140, que incluye una sección sobre la cooperación entre los sectores público y privado, se dan orientaciones sobre buenas prácticas. La financiación con cargo al Fondo de Seguridad Interior-Policía se centra especialmente en la mejora de la cooperación entre los sectores público y privado.

amenazas internas. Un aspecto importante que se ha de reflejar es el hecho de que las minorías y las personas vulnerables pueden verse afectadas desproporcionadamente —incluidas las personas objeto de ataques por su religión o su género— y, por lo tanto, requieren una atención especial. Las autoridades públicas regionales y locales desempeñan un papel importante en la mejora de la seguridad de los espacios públicos. La Comisión también está ayudando a fomentar la innovación de las ciudades en materia de seguridad en los espacios públicos[55]. La puesta en marcha de una nueva asociación de la Agenda Urbana[56] sobre «seguridad en los espacios públicos» en noviembre de 2018 refleja el firme compromiso de los Estados miembros, la Comisión y las ciudades de contrarrestar mejor las amenazas para la seguridad en el espacio urbano.

El mercado de los **drones** sigue creciendo, con muchos usos valiosos y legítimos. Sin embargo, también pueden ser objeto de abusos por parte de delincuentes y terroristas y suponen una especial amenaza para los espacios públicos. Entre los objetivos pueden figurar los individuos, las concentraciones de personas, las infraestructuras críticas, las autoridades policiales, las fronteras o los espacios públicos. Los conocimientos sobre el uso de drones en el marco de conflictos podrían acabar abriéndose camino hasta Europa, ya sea directamente (a través de los combatientes terroristas extranjeros que regresan) o en línea. Las normas ya elaboradas por la Agencia Europea de Seguridad Aérea constituyen un primer paso importante en ámbitos como el registro de operadores de drones y la identificación remota obligatoria de drones. Al ser los drones cada vez más fáciles de conseguir, más asequibles y más capaces, resultan necesarias medidas adicionales. Esto podría incluir el intercambio de información, la orientación y las buenas prácticas para su uso generalizado, incluidos los cuerpos y fuerzas de seguridad del Estado, así como más ensayos de contramedidas para los drones[57]. Además, las implicaciones en materia de privacidad y protección de datos del uso de drones en los espacios públicos deben seguir analizándose y abordándose.

Medidas clave

- Legislación sobre la protección y la resiliencia de las infraestructuras críticas
- Revisión de la Directiva sobre Ciberseguridad
- Una iniciativa sobre la resiliencia operativa del sector financiero
- Protección y ciberseguridad de las infraestructuras energéticas críticas y del código de red sobre ciberseguridad para los flujos eléctricos transfronterizos
- Una Estrategia de Ciberseguridad Europea
- Próximos pasos para la creación de una unidad informática conjunta
- Normas comunes en materia de seguridad de la información y ciberseguridad para las instituciones, los órganos y los organismos de la UE
- Intensificación de la cooperación para la protección de los espacios públicos, incluidos los lugares de culto
- Intercambio de buenas prácticas para la lucha contra el uso indebido de drones

[55] Tres ciudades (El Pireo en Grecia, Tampere en Finlandia y Turín en Italia) probarán nuevas soluciones como parte de las Acciones Innovadoras Urbanas, cofinanciadas por el Fondo Europeo de Desarrollo Regional (FEDER).

[56] La Agenda Urbana para la UE representa un nuevo método de trabajo multinivel que fomenta la cooperación entre los Estados miembros, las ciudades, la Comisión Europea y otras partes interesadas para estimular el crecimiento, la calidad de vida y la innovación en las ciudades de Europa y para detectar y hacer frente con éxito a los retos sociales.

[57] Recientemente se ha puesto en marcha un programa plurianual de ensayo para ayudar a los Estados miembros a desarrollar una metodología común y una plataforma de ensayo en este ámbito.

2. Hacer frente a las amenazas cambiantes

Ciberdelincuencia

La tecnología ofrece nuevas oportunidades a la sociedad. Asimismo, aporta nuevos instrumentos a la administración de justicia y las fuerzas y cuerpos de seguridad. Pero, al mismo tiempo, abre puertas a los delincuentes. Van en aumento los programas maliciosos, el robo de datos personales o empresariales mediante el pirateo informático y la interrupción de la actividad digital causante de daños financieros o de reputación. El entorno resiliente creado por una ciberseguridad sólida constituye la primera defensa. Las autoridades policiales deben estar en condiciones de trabajar en el ámbito de las investigaciones digitales con normas claras para investigar y perseguir los delitos y ofrecer a las víctimas la protección necesaria. Este trabajo debe basarse en el *Joint Cybercrime Action Task Force* (Grupo de Acción Conjunta contra la Ciberdelincuencia) de Europol y en el Protocolo de respuesta policial ante emergencias creado para coordinar la respuesta a los ciberataques a gran escala. Los mecanismos efectivos que permiten las asociaciones y la cooperación entre los sectores público y privado también son fundamentales.

Paralelamente, la lucha contra la ciberdelincuencia debe convertirse en una prioridad estratégica de comunicación en toda la UE a fin de alertar a los europeos respecto de los riesgos y las medidas preventivas que podrían adoptar. Esto debería formar parte de un enfoque proactivo. Un paso esencial es también la plena aplicación del marco jurídico vigente[58]: la Comisión no dudará en incoar procedimientos de infracción según proceda, así como a seguir revisando este marco para garantizar que siga siendo adecuado para los fines perseguidos. La Comisión también estudiará, junto con Europol y la Agencia de la UE para la Ciberseguridad (ENISA), la viabilidad de un sistema de alerta rápida de la UE para la ciberdelincuencia que podría garantizar el flujo de información y las reacciones rápidas en caso de aumento repentino de los ciberdelitos.

La ciberdelincuencia es un desafío mundial respecto del que es necesaria una cooperación internacional eficaz. La UE apoya el Convenio de Budapest sobre la Ciberdelincuencia del Consejo de Europa, que constituye un marco eficaz y consolidado que permite a todos los países determinar qué sistemas y canales de comunicación necesitan crear para poder colaborar eficazmente entre sí.

A casi la mitad de los ciudadanos de la UE les preocupa mucho el uso indebido de datos[59] y la **usurpación de identidad**[60]. El uso fraudulento de identidades con ánimo de lucro es un aspecto, pero también puede darse un impacto personal y psicológico importante, ya que las publicaciones ilegales realizadas por un usurpador de identidad pueden permanecer en línea durante años. La Comisión estudiará posibles medidas prácticas para proteger a las víctimas de cualquier forma de usurpación de identidad, teniendo en cuenta la próxima iniciativa de Identidad Digital Europea[61].

---

[58] Directiva 2013/40/UE relativa a los ataques contra los sistemas de información.

[59] 46 % (Eurobarómetro sobre las actitudes de los europeos respecto de la ciberseguridad, enero de 2020).

[60] La inmensa mayoría de los encuestados para el Eurobarómetro «Europeans' attitudes towards Internet security» (Actitudes de los europeos respecto de la seguridad en internet) de 2018 —el 95 %— consideraba que la usurpación de identidad constituye un delito grave, y siete de cada diez afirmaban que es un delito muy grave. El Eurobarómetro publicado en enero de 2020 confirmó la preocupación en torno a la ciberdelincuencia, el fraude en línea y la usurpación de identidad: dos tercios de los encuestados se mostraban preocupados por el fraude bancario (67 %) o la usurpación de identidad (66 %).

[61] Comunicación de 19 de febrero de 2020 «Configurar el Futuro Digital de Europa» [COM(2020) 67].

Hacer frente a la ciberdelincuencia significa mirar hacia delante. A medida que la sociedad utiliza nuevos avances tecnológicos para fortalecer la economía y la sociedad, los delincuentes también pueden intentar aprovechar estas herramientas con fines negativos. Por ejemplo, los delincuentes pueden valerse de la inteligencia artificial para detectar e identificar contraseñas o para simplificar la creación de programas maliciosos a fin de aprovechar imágenes y audio que puedan utilizarse después para la usurpación de identidad o el fraude.

Una aplicación de la ley moderna

Los profesionales de la policía y la administración de justicia necesitan adaptarse a las nuevas tecnologías. Los avances tecnológicos y las amenazas emergentes exigen que las autoridades policiales tengan acceso a nuevos instrumentos, adquieran nuevas capacidades y desarrollen técnicas de investigación alternativas. Para complementar las medidas legislativas destinadas a mejorar el acceso transfronterizo a las pruebas electrónicas en el marco de las investigaciones penales, la UE puede ayudar a las autoridades policiales a desarrollar las capacidades necesarias para detectar, proteger y leer los datos necesarios para investigar los delitos y a utilizar dichos datos como pruebas ante los tribunales. La Comisión estudiará medidas para **mejorar la capacidad para hacer aplicar la ley en las investigaciones digitales**, definiendo cómo hacer el mejor uso posible de la investigación y el desarrollo para crear nuevos instrumentos de aplicación de la ley; y la manera en que la formación puede ofrecer las capacidades adecuadas a las fuerzas y cuerpos de seguridad y a la administración de justicia. Esto incluirá también la puesta a disposición de evaluaciones científicas y métodos de ensayo rigurosos a través del Centro Común de Investigación de la Comisión.

Los enfoques comunes también pueden garantizar que la **inteligencia artificial, las capacidades espaciales, los macrodatos** y la **informática de alto rendimiento** se integren en la política de seguridad de manera eficaz tanto en la lucha contra los delitos como en la garantía de los derechos fundamentales. La inteligencia artificial podría actuar como un potente instrumento para luchar contra la delincuencia, creando enormes capacidades de investigación mediante el análisis de grandes cantidades de información y detectando pautas y anomalías[62]. También puede proporcionar instrumentos concretos para, por ejemplo, ayudar a identificar contenidos terroristas en línea, descubrir transacciones sospechosas en las ventas de productos peligrosos u ofrecer asistencia a los ciudadanos en situaciones de emergencia. El aprovechamiento efectivo de este potencial implica combinar la investigación, la innovación y los usuarios de inteligencia artificial con la gobernanza y las infraestructuras técnicas adecuadas, implicando activamente al sector privado y al mundo académico. Requiere también garantizar las normas más exigentes en materia de respeto de los derechos fundamentales, garantizando al mismo tiempo una protección eficaz de los ciudadanos. En particular, las decisiones que afecten a particulares deben estar sujetas a supervisión humana y cumplir la legislación pertinente de la UE[63].

Se necesitan información y pruebas electrónicas en alrededor del 85 % de las investigaciones de delitos graves, y el 65 % del total de las solicitudes se dirigen a

[62] Por ejemplo, en los delitos financieros.

[63] Esto implica el cumplimiento de la legislación vigente, incluidos el Reglamento (UE) 2016/679, General de Protección de Datos, y la Directiva (UE) 2016/680 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales.

proveedores establecidos en otra jurisdicción[64]. El hecho de que los rastros físicos tradicionales hayan pasado a encontrarse en línea amplía aún más la brecha entre las fuerzas y cuerpos de seguridad y las capacidades de los delincuentes. Es esencial establecer normas claras para el acceso transfronterizo a las pruebas electrónicas en las investigaciones penales. Esta es la razón por la que una adopción rápida por parte del Parlamento Europeo y el Consejo de las propuestas sobre pruebas electrónicas es clave para proporcionar a los profesionales un instrumento eficaz. El acceso transfronterizo a las pruebas electrónicas mediante negociaciones internacionales multilaterales y bilaterales también es clave para establecer normas compatibles a nivel internacional[65].

El **acceso a las pruebas digitales** también depende de la disponibilidad de la información. Si los datos se eliminan con demasiada rapidez, pueden desaparecer pruebas importantes, de modo que ya no exista la posibilidad de identificar y localizar a los sospechosos y a las redes delictivas (así como a las víctimas). Por otra parte, los sistemas de conservación de datos plantean problemas de protección de la privacidad. En función de los resultados de los asuntos pendientes ante el Tribunal de Justicia Europeo, la Comisión evaluará el camino a seguir en materia de conservación de datos.

El acceso a la información de registros de nombres de dominio en internet (datos WHOIS)[66] es importante para las investigaciones penales, la ciberseguridad y la protección de los consumidores. Sin embargo, el acceso a esta información es cada vez más difícil, a la espera de la adopción de una nueva política WHOIS por la Corporación para la Asignación de Nombres y Números en Internet (ICANN). La Comisión seguirá trabajando con la ICANN y la comunidad multilateral para garantizar que los solicitantes de acceso legítimos, incluidas las fuerzas y cuerpos de seguridad, cuenten con un acceso eficaz a los datos WHOIS en consonancia con la normativa internacional y de la UE en materia de protección de datos. Esto abarcará la evaluación de las soluciones potenciales, incluida la posibilidad de que sea necesario legislar para aclarar las normas de acceso a dicha información.

Las autoridades policiales y judiciales también deben estar equipadas para obtener los datos y las pruebas necesarios una vez que la **arquitectura 5G para las telecomunicaciones móviles** esté plenamente implantada en la UE, de una forma que respete la confidencialidad de las comunicaciones. La Comisión apoyará un planteamiento reforzado y coordinado de cara a la elaboración de normas internacionales, la definición de mejores prácticas, el proceso, la interoperabilidad técnica en ámbitos tecnológicos clave como la IA, la internet de las cosas o las tecnologías de cadena de bloques.

Actualmente, una parte sustancial de las investigaciones contra todas las formas de delincuencia y terrorismo implican **información cifrada**. El cifrado es esencial para el mundo digital, pues asegura los sistemas y las transacciones digitales y protege una serie de derechos fundamentales, entre ellos la libertad de expresión, la privacidad y la protección de datos. Sin embargo, si se utiliza con fines delictivos también puede ocultar la identidad de los delincuentes y el contenido de sus comunicaciones. La Comisión estudiará y apoyará soluciones equilibradas desde el punto de vista técnico, operativo y jurídico a los desafíos y promoverá un enfoque que mantenga la eficacia del cifrado a la hora de proteger la

[64] Documento de trabajo de los servicios de la Comisión SWD(2018) 118 final.

[65] En particular, el Segundo Protocolo Adicional del Convenio sobre la Ciberdelincuencia de Budapest del Consejo de Europa y un acuerdo entre la UE y los Estados Unidos sobre el acceso transfronterizo a las pruebas electrónicas.

[66] Almacenada en bases de datos mantenidas por 2 500 registradores y operadores de registradores ubicados por todo el mundo.

privacidad y la seguridad de las comunicaciones, y que aporte al mismo tiempo una respuesta eficaz contra la delincuencia y el terrorismo.

Lucha contra los contenidos ilícitos en línea

Armonizar la seguridad de los entornos en línea y físicos significa seguir avanzando en la **lucha contra los contenidos ilícitos en línea**. Cada vez más, las amenazas fundamentales que acechan a los ciudadanos, como el terrorismo, el extremismo o el abuso sexual de menores, dependen del entorno digital: ello exige acciones concretas y un marco para garantizar el respeto de los derechos fundamentales. Un primer paso esencial es concluir rápidamente las negociaciones en torno a la propuesta de legislación relativa a los contenidos terroristas en línea[67] y garantizar su aplicación. El refuerzo de la cooperación voluntaria entre las fuerzas y cuerpos de seguridad y el sector privado en el seno del **Foro de la UE sobre Internet** es también clave para luchar contra el uso indebido de internet por parte de terroristas, extremistas violentos y delincuentes. La Unidad de Notificación de Contenidos de Internet de la UE en Europol seguirá desempeñando un papel crucial en el seguimiento de la actividad de los grupos terroristas en línea y de las medidas adoptadas por las plataformas[68], así como en el desarrollo del **Protocolo de crisis de la UE**[69]. Además, la Comisión seguirá colaborando con otros socios internacionales para dar una respuesta a escala mundial a estos retos, en particular mediante la participación en el **Foro Mundial de Internet de lucha contra el terrorismo**. Se seguirá trabajando para apoyar el desarrollo de discursos que argumenten en contra de estos contenidos ilícitos y de discursos alternativos a través del Programa de Empoderamiento de la Sociedad Civil[70].

Con el fin de prevenir y combatir la propagación de la incitación ilegal al odio en línea, la Comisión puso en marcha en 2016 el Código de Conducta para la Lucha contra la Incitación Ilegal al Odio en Internet, con un compromiso voluntario de las plataformas en línea para eliminar los contenidos de incitación al odio. La evaluación más reciente muestra que las empresas evalúan el 90 % de los contenidos señalados en un plazo de 24 horas y eliminan el 71 % de los que consideran como de incitación ilegal al odio. Sin embargo, las plataformas deben mejorar la transparencia y la información a los usuarios y garantizar una evaluación coherente de los contenidos señalados[71].

El Foro de la UE sobre Internet también facilitará los intercambios sobre las tecnologías existentes y en desarrollo para hacer frente a los desafíos relacionados con el abuso sexual de menores en línea. La respuesta al abuso sexual de menores en línea constituye una parte central de una nueva estrategia para intensificar la **lucha contra el abuso sexual de menores**[72], que intentará maximizar el uso de las herramientas disponibles a nivel de la UE para luchar contra estos delitos. Las empresas deben poder continuar su trabajo para detectar y eliminar los materiales en línea relacionados con el abuso sexual de menores, y los perjuicios causados por estos materiales requieren un marco que establezca obligaciones claras y permanentes para abordar el problema. La Estrategia también anunciará que la

---

67 Propuesta para la prevención de la difusión de contenidos terroristas en línea, COM(2018) 640 de 12 de septiembre de 2018.

68 Europol, noviembre de 2019.

69 Una Europa que protege - Protocolo de crisis de la UE: responder a los contenidos terroristas en línea (octubre de 2019).

70 En relación con el trabajo del Programa para la Sensibilización frente a la Radicalización, véase la sección IV.3.

71 https://ec.europa.eu/info/sites/info/files/codeofconduct_2020_factsheet_12.pdf

72 EU strategy for a more effective fight against child sexual abuse (Estrategia de la UE para una lucha más efectiva contra el abuso sexual de menores), COM(2020) 607.

Comisión empezará a preparar una legislación sectorial específica para hacer frente a los abusos sexuales de menores en línea de forma más eficaz, con pleno respeto de los derechos fundamentales.

De manera más general, la futura norma sobre servicios digitales también aclarará y mejorará las normas de responsabilidad y seguridad de los mismos y eliminará los desincentivos que frenan la lucha contra contenidos, bienes o servicios ilegales.

Además, la Comisión seguirá colaborando con los socios internacionales y con el **Foro Mundial de Internet de lucha contra el terrorismo**, en particular a través del comité consultivo independiente, para debatir el modo de abordar estos desafíos a nivel mundial preservando los valores de la UE y los derechos fundamentales. También deberían tratarse nuevos temas, como el de los algoritmos o los juegos en línea[73].

Amenazas híbridas

La magnitud y diversidad de las actuales amenazas híbridas no tienen precedentes. La crisis de la COVID-19 ha venido también a demostrarlo, con el intento de instrumentalización de la pandemia por parte de diversos agentes estatales y no estatales, en particular mediante la manipulación del entorno informativo y el ataque de infraestructuras básicas. Esto puede debilitar la cohesión social y socavar la confianza en las instituciones de la UE y en los gobiernos de los Estados miembros.

El enfoque de la UE con respecto a las amenazas híbridas se recoge en el Marco Conjunto de 2016[74] y en la Comunicación conjunta de 2018 sobre el refuerzo de la resiliencia híbrida[75]. La acción a nivel de la UE se sustenta en una considerable caja de herramientas que cubre el nexo entre la dimensión interior y exterior, sobre la base de un planteamiento de la sociedad en su conjunto y en estrecha cooperación con socios estratégicos, en particular la OTAN y el G7. Acompañando a esta Estrategia se publica un informe sobre la aplicación del enfoque de la UE para hacer frente a las amenazas híbridas[76]. Sobre la base de la cartografía[77] presentada en paralelo a la presente Estrategia, los servicios de la Comisión y el Servicio Europeo de Acción Exterior crearán una **plataforma en línea restringida** para la referencia de los Estados miembros a los instrumentos y medidas de lucha contra las amenazas híbridas a escala de la UE.

Si bien la responsabilidad de la lucha contra las amenazas híbridas recae en primer lugar en los Estados miembros —debido a los vínculos intrínsecos con las políticas de seguridad y de defensa nacionales— ciertas vulnerabilidades son comunes a todos los Estados miembros y determinadas amenazas desbordan sus fronteras, como las que tienen por objetivo redes o infraestructuras transfronterizas. La Comisión y el Alto Representante establecerán un enfoque de la UE para las amenazas híbridas que integre las dimensiones externa e interna

[73] Los terroristas usan cada vez más el sistema de mensajería de las plataformas de juego para sus comunicaciones y los jóvenes terroristas replican ataques violentos de videojuegos.

[74] Comunicación conjunta sobre la lucha contra las amenazas híbridas – Una respuesta de la Unión Europea, JOIN(2016) 18.

[75] Aumentar la resiliencia y desarrollar las capacidades para hacer frente a las amenazas híbridas, JOIN(2018) 16.

[76] SWD(2020) 153, Informe sobre la aplicación de la Comunicación conjunta sobre la lucha contra las amenazas híbridas de 2016 y la Comunicación conjunta «Aumentar la resiliencia y desarrollar las capacidades para hacer frente a las amenazas híbridas», de 2018

[77] SWD (2020) 152, Cartografía de las medidas relacionadas con el incremento de la resiliencia y la lucha contra las amenazas híbridas.

en un flujo continuo y fusione las consideraciones nacionales y de la UE . Debe cubrirse el espectro de acción en su totalidad, desde la detección precoz, el análisis, la sensibilización, la resiliencia y la prevención hasta la respuesta a las crisis y la gestión de las consecuencias.

Además del refuerzo en la aplicación, y teniendo en cuenta la constante evolución de las amenazas híbridas, se hará especial hincapié en **la integración de las consideraciones en materia de amenazas híbridas en la formulación de todas las políticas**, a fin de estar al día de los cambios dinámicos que se registran y garantizar que se tienen en cuenta todas las iniciativas potencialmente pertinentes. También se evaluarán a la luz de las cuestiones relacionadas con las amenazas híbridas los efectos de nuevas iniciativas, incluidas las iniciativas en ámbitos que hasta ahora no son competencia del marco sobre las amenazas híbridas, como la educación, la tecnología y la investigación. Este enfoque puede aprovechar el trabajo realizado de conceptualización de las amenazas híbridas, que permite una visión global de las distintas herramientas que pueden utilizar los adversarios[78]. El objetivo debe ser garantizar que el proceso de toma de decisiones se apoye en los informes periódicos, completos y basados en los datos que aporten los servicios de inteligencia sobre la evolución de las amenazas híbridas. Esto dependerá en gran medida de los servicios de inteligencia de los Estados miembros y de la intensificación de la cooperación en materia de inteligencia con los servicios competentes de los Estados miembros a través del INTCEN de la UE.

Para mejorar el **conocimiento de la situación**, los servicios de la Comisión y el Servicio Europeo de Acción Exterior estudiarán la forma de racionalizar los flujos de información procedentes de distintas fuentes, incluidos los Estados miembros, así como de agencias de la UE como ENISA, Europol y Frontex. La Célula de Fusión de la UE contra las amenazas híbridas seguirá siendo el punto focal de la UE para la evaluación de estas amenazas. El **refuerzo de la resiliencia** es fundamental para prevenir las amenazas híbridas y ofrecer protección. Por lo tanto, se impone un seguimiento sistemático y una medición objetiva de los avances en este ámbito. Un primer paso será identificar las bases de referencia sectoriales sobre resiliencia híbrida tanto para los Estados miembros como para las instituciones y organismos de la UE. Por último, para reforzar la **preparación frente a las crisis híbridas**, debe revisarse el protocolo existente («EU Playbook» de 2016[79]), de modo que refleje la revisión más amplia y el refuerzo del sistema de respuesta de la UE a la crisis actualmente en estudio[80]. El objetivo es maximizar el efecto de la acción de la UE, agrupando rápidamente las respuestas sectoriales y garantizando una cooperación sin fisuras con nuestros socios, y en primer lugar con la OTAN.

Acciones clave
• Garantizar la aplicación de la legislación en materia de ciberdelincuencia y su adecuación al objetivo previsto • Elaborar una estrategia para una lucha más eficaz contra los abusos sexuales de menores • Presentar propuestas sobre la detección y la eliminación de material relacionado con el abuso sexual de menores

[78] Panorama de las amenazas híbridas: modelo conceptual, JRC117280, desarrollado conjuntamente por el Centro Común de Investigación y el Centro de Excelencia para la Lucha contra las Amenazas Híbridas.

[79] Protocolo operativo de la UE para la lucha contra las amenazas híbridas («EU Playbook»), SWD(2016) 227.

[80] A raíz de su videoconferencia del 26 de marzo de 2020, los miembros del Consejo Europeo adoptaron una Declaración sobre las acciones de la UE en respuesta al brote de CODVID-19, en la que se invitaba a la Comisión a hacer propuestas para un sistema de gestión de crisis más ambicioso y de mayor alcance en el seno de la UE.

- Concebir un enfoque de la UE para la lucha contra las amenazas híbridas.
- Revisar el protocolo operativo de la UE para la lucha contra las amenazas híbridas («EU Playbook»)
- Evaluar la manera de mejorar la capacidad de los cuerpos y fuerzas de seguridad por lo que se refiere a las investigaciones digitales

3. Proteger a los europeos frente al terrorismo y la delincuencia organizada

Terrorismo y radicalización

La amenaza terrorista en la UE sigue siendo alta. Aunque el número total de atentados haya disminuido, estos pueden tener un efecto devastador. La radicalización también puede contribuir a polarizar y a desestabilizar la cohesión social. Los Estados miembros siguen siendo los principales responsables de la lucha contra el terrorismo y la radicalización. No obstante, la cada vez mayor dimensión transfronteriza y multisectorial de esta amenaza exige nuevos pasos en la cooperación y coordinación en el seno de la UE. La aplicación efectiva de la legislación antiterrorista de la UE, incluidas las medidas restrictivas[81], es prioritaria. La ampliación del mandato de la Fiscalía Europea a los delitos de terrorismo transfronterizos sigue siendo un objetivo.

La lucha contra el terrorismo empieza por abordar las causas profundas. La polarización de la sociedad, la discriminación real o percibida y otros factores psicológicos y sociológicos pueden hacer más fácil que ciertas personas sucumban ante discursos radicales. En este contexto, la lucha contra la **radicalización** ha de ir de la mano del fomento de la cohesión social a nivel local, nacional y europeo. En la última década se han desarrollado varias iniciativas y políticas de impacto, como la Red de la UE para la Sensibilización frente a la Radicalización y la iniciativa Ciudades de la UE contra la Radicalización[82]. Ha llegado el momento de estudiar la forma de racionalizar las políticas, las iniciativas y los fondos de la UE para hacer frente a la radicalización. Estas acciones pueden apoyar el desarrollo de capacidades y conocimientos, mejorar la cooperación, reforzar la base empírica y ayudar a evaluar el progreso, con la participación de todas las partes interesadas pertinentes, incluidos los profesionales de primera línea, los responsables políticos y el mundo académico[83]. Las políticas blandas, como las de educación, cultura, juventud y deporte, podrían contribuir a la prevención de la radicalización, ofreciendo oportunidades para la juventud en situación de riesgo y mejorando la cohesión en el seno de la UE[84]. Los ámbitos prioritarios incluyen el trabajo en materia de detección precoz, la gestión de riesgos, el aumento de la resiliencia y la desmovilización, así como la rehabilitación y la reintegración en la sociedad.

Los terroristas han tratado de adquirir materiales **químicos, biológicos, radiológicos y nucleares** (QBRN)[85] y de desarrollar sus conocimientos y capacidad para utilizarlos como

[81] El Consejo ha adoptado medidas restrictivas con respecto al EIIL (Daesh) y Al Qaeda, así como medidas restrictivas específicas dirigidas a determinadas personas y entidades con el fin de luchar contra el terrorismo. Véase el mapa de sanciones de la UE (https://www.sanctionsmap.eu/#/main) para tener una visión general de todas las medidas restrictivas.

[82] La iniciativa piloto «Ciudades de la UE contra la Radicalización» tiene el doble objetivo de fomentar el intercambio de conocimientos entre las ciudades de la UE y recabar opiniones sobre la mejor manera de apoyar a las comunidades locales a nivel de la UE.

[83] Por ejemplo, la financiación en el marco del Fondo Europeo de Seguridad y del programa Ciudadanía.

[84] Acciones de la UE como los intercambios virtuales de Erasmus+ o el hermanamiento electrónico.

[85] En los últimos dos años se han producido varios casos, tanto en Europa (Francia, Alemania, Italia) como en otros países (Túnez, Indonesia) de ataques con agentes biológicos (generalmente toxinas vegetales).

armas[86]. En la propaganda terrorista se destaca el potencial de los ataques QBRN. Un potencial de destrucción tan alto exige una especial atención. Partiendo del enfoque utilizado para regular el acceso a los precursores de explosivos, la Comisión estudiará la posibilidad de restringir el acceso a determinados productos químicos peligrosos que podrían utilizarse para perpetrar atentados. El desarrollo de las capacidades de respuesta de la UE en materia de protección civil (rescEU) en el ámbito QBRN también será fundamental. La cooperación con terceros países también es importante para mejorar una cultura común de seguridad y protección QBRN, utilizando plenamente los centros de excelencia QBRN de la UE. Esta cooperación incluirá las diferencias nacionales y las evaluaciones de riesgo, el apoyo a los planes de acción nacionales y regionales en materia de QBRN, los intercambios de buenas prácticas y las actividades de desarrollo de capacidades QBRN.

La UE ha desarrollado la legislación más avanzada del mundo para restringir el acceso a los **precursores de explosivos**[87] y detectar transacciones sospechosas destinadas a fabricar artefactos explosivos improvisados. Pero la amenaza de los explosivos de fabricación casera sigue siendo elevada, y estos han sido utilizados en múltiples ataques en toda la UE[88]. El primer paso debe ser la aplicación de las normas, así como garantizar que el entorno en línea no permita eludir los controles.

El enjuiciamiento efectivo de quienes han cometido delitos terroristas, incluidos los **combatientes terroristas extranjeros** en la actualidad en Siria e Irak, es también un elemento importante de la política de lucha contra el terrorismo. Aunque estas cuestiones son abordadas principalmente por los Estados miembros, la coordinación y el apoyo de la UE pueden ayudarles a responder a estos desafíos comunes. Un avance importante vendrá de la mano de las medidas en curso para aplicar íntegramente la legislación en materia de seguridad de las fronteras[89] y hacer pleno uso de todas las bases de datos pertinentes de la UE para compartir información sobre sospechosos conocidos. La identificación de las personas de alto riesgo ha de ir acompañada de una política de reintegración y rehabilitación. La cooperación entre profesionales, incluido el personal de los centros penitenciarios y la libertad vigilada, reforzará la comprensión judicial de los procesos de radicalización hacia el extremismo violento y el enfoque del sector judicial por lo que se refiere a las penas y a las alternativas al internamiento.

El reto que plantean los combatientes terroristas extranjeros es ilustrativo de la relación entre **seguridad** interior y **exterior**. La cooperación en materia de lucha contra el terrorismo y de prevención y lucha contra la radicalización y el extremismo violento es fundamental para la seguridad en la UE[90]. Es necesario adoptar nuevas medidas para desarrollar las asociaciones antiterroristas y la cooperación con los países de la vecindad y más allá, aprovechando la experiencia de la Red de expertos en seguridad y lucha contra el terrorismo de la UE. El plan de acción conjunta en materia de lucha contra el terrorismo en los Balcanes Occidentales es una buena referencia para dicha cooperación específica. En particular, debe

---

86 El Consejo adoptó medidas restrictivas contra la proliferación y el uso de las armas químicas.

87 Productos químicos que podrían utilizarse de manera indebida para fabricar explosivos caseros. Regulados a través del Reglamento (UE) 2019/1148 de 2019 sobre la comercialización y la utilización de precursores de explosivos.

88 Algunos ejemplos de estos ataques devastadores son los perpetrados en Oslo (2011), París (2015), Bruselas (2016) y Manchester (2017). Un atentado con un explosivo casero en Lyon (2019) causó 13 heridos.

89 Incluido el nuevo mandato de la Agencia Europea de la Guardia de Fronteras y Costas (Frontex).

90 Las Conclusiones del Consejo de 16 de junio de 2020 subrayaron la necesidad de proteger a los ciudadanos de la UE contra el terrorismo y el extremismo violento en todas sus formas y con independencia de su origen, y de seguir reforzando el compromiso y la acción de la UE en la lucha contra el terrorismo en determinados ámbitos geográficos y temáticos prioritarios.

trabajarse por reforzar la capacidad de los países socios de identificar y localizar a combatientes terroristas extranjeros. La UE también seguirá promoviendo la cooperación multilateral trabajando con los principales actores mundiales en este ámbito, como las Naciones Unidas, la OTAN, el Consejo de Europa, Interpol y la OSCE. También colaborará con el Foro Mundial contra el Terrorismo y la Coalición Mundial contra el Daesh, así como con los agentes pertinentes de la sociedad civil. Los instrumentos de política exterior de la Unión, incluidos los correspondientes al desarrollo y la cooperación, también desempeñan un papel importante a la hora de trabajar con terceros países para prevenir el terrorismo y la piratería. La cooperación internacional también es esencial para cortar todas las fuentes de **financiación del terrorismo**, por ejemplo, a través del Grupo de Acción Financiera Internacional.

Delincuencia organizada

La delincuencia organizada tiene un enorme coste económico y personal. Se calcula que la pérdida económica debida a la delincuencia organizada y a la corrupción representa entre 218 000 y 282 000 millones de euros al año[91]. En 2017 se investigó en Europa a más de 5 000 grupos de delincuencia organizada, lo que supone un aumento del 50 % con respecto a 2013[92]. La delincuencia organizada opera cada vez más de forma transfronteriza, incluso desde la vecindad inmediata de la UE, lo que exige que se intensifique la cooperación operativa y el intercambio de información con los socios de la vecindad.

Están surgiendo nuevos retos a través de la delincuencia en línea: la pandemia de COVID-19 ha traído consigo un aumento importante de las estafas en línea a grupos vulnerables, y los productos sanitarios han sido objeto de robos[93]. La UE debe intensificar su trabajo contra la delincuencia organizada, también a escala internacional, dotándose de más herramientas para desmantelar el modelo de negocio de este tipo de delincuencia. La lucha contra la delincuencia organizada requiere también una estrecha cooperación con las administraciones locales y regionales, así como con la sociedad civil, socios clave en la prevención de la delincuencia y en la prestación de asistencia y apoyo a las víctimas, con una necesidad particular entre las administraciones en las regiones fronterizas. Este trabajo se reunirá en una **agenda de lucha contra la delincuencia organizada**.

Más de un tercio de los grupos de delincuencia organizada activos en la UE participan en la producción, el tráfico o la distribución de drogas. La adicción a las drogas provocó más de 8 000 muertes por sobredosis en la UE en 2019. La mayor parte del **tráfico de drogas** se lleva a cabo a través de las fronteras y gran parte de los beneficios que genera se infiltran en la economía legal[94]. Una nueva agenda de la UE de lucha contra la droga[95] incrementará los esfuerzos de la UE y de los Estados miembros por reducir la oferta y la demanda de drogas, definir acciones conjuntas que aborden este problema común y reforzar el diálogo y la cooperación entre la UE y los socios externos en cuestiones relacionadas con las drogas. Tras una evaluación del Observatorio Europeo de las Drogas y las Toxicomanías, la Comisión evaluará si es necesario actualizar su mandato para hacer frente a nuevos desafíos.

---

91 En términos de producto interior bruto (PIB); Informes de Europol: «Does crime still pay? – Criminal asset recovery in the EU» (¿Sigue resultando provechoso el delito? Recuperación de activos delictivos en la UE), de 2016.

92 Europol, Evaluaciones de las amenazas de la delincuencia grave y organizada (SOCTA, por sus siglas en inglés), 2013 y 2017.

93 Europol, 2020.

94 Informe sobre los mercados de la droga en la UE de 2019, elaborado conjuntamente por el EMCDDA y Europol. (Noviembre de 2019).

95 Agenda y plan de acción de lucha contra la droga de la UE 2021-2025 [COM(2020) 606].

Los grupos de la delincuencia organizada y los terroristas también son agentes clave en el comercio de **armas de fuego ilegales**. Entre 2009 y 2018 se produjeron 23 incidentes de tiroteo masivo en Europa en los que perdieron la vida más de 340 personas[96]. Con frecuencia, el tráfico de armas de fuego en la UE procede de su vecindad[97]. Esto apunta a la necesidad de reforzar la coordinación y la cooperación tanto dentro de la UE como con los socios internacionales, en particular Interpol, para armonizar la recogida de información e informar sobre las incautaciones de armas de fuego. Asimismo es esencial mejorar la trazabilidad de las armas, también en Internet, y garantizar el intercambio de información entre las autoridades responsables de la concesión de licencias y las policiales. La Comisión va a presentar un nuevo **plan de acción de la UE contra el tráfico de armas de fuego**[98] y evaluará también si las normas relativas a la autorización de la exportación y las medidas dirigidas al tránsito y la importación de armas de fuego siguen ajustándose a los fines perseguidos[99].

Las organizaciones delictivas tratan como mercancía a los migrantes y a las personas necesitadas de protección internacional. El 90 % de los migrantes irregulares que llegan a la UE consiguen hacerlo a través de una red delictiva[100]. El tráfico ilícito de migrantes a menudo está también interrelacionado con otras formas de delincuencia organizada, como la trata de seres humanos[101]. Al margen del enorme coste humano de estas prácticas, Europol estima que, globalmente, el beneficio anual generado por todas las formas de explotación de la trata de seres humanos asciende a 29 400 millones de euros. Se trata de un delito transnacional que se alimenta de la demanda ilegal de dentro y fuera de la UE y afecta a todos los Estados miembros. Los escasos logros en materia de detección, procesamiento y condena de estos delitos exigen la adopción de un nuevo enfoque para intensificar la acción. Un nuevo **enfoque global de la trata de seres humanos** permitirá unificar las líneas de actuación. Además, la Comisión presentará un **nuevo Plan de Acción de la UE contra el tráfico ilícito de migrantes** para el período 2021-2025 Ambos frentes de actuación se centrarán en la lucha contra las redes delictivas, el impulso de la cooperación y el apoyo a la labor de los cuerpos y fuerzas de seguridad.

Los grupos de delincuencia organizada y los terroristas también buscan oportunidades en otros ámbitos, especialmente los que generan altos beneficios con un bajo riesgo de detección, como los **delitos contra el medio ambiente**. La caza y el comercio ilícitos de fauna silvestre, la extracción minera y la tala ilegales y la eliminación y el transporte ilegales de residuos, se han convertido en el cuarto negocio delictivo más importante en todo el mundo[102]. También se ha registrado una explotación delictiva de los regímenes de comercio de derechos de emisión y de los sistemas de certificación energética, así como un uso indebido de la financiación asignada a la resiliencia medioambiental y el desarrollo

[96] Instituto Flamenco de la Paz, Armed to kill (Armados para matar) (Octubre de 2019).

[97] La UE ha financiado la lucha contra la proliferación y el tráfico de armas ligeras y de pequeño calibre en la región desde 2002; en particular, financia la red de expertos en armas de fuego de Europa Sudoriental (SEEFEN). Desde 2019, los socios de los Balcanes Occidentales han participado plenamente en la prioridad sobre armas de fuego de la plataforma multidisciplinar europea contra las amenazas delictivas (EMPACT).

[98] COM(2020) 608.

[99] Reglamento (UE) n.º 258/2012, por el que se aplica el artículo 10 del Protocolo de las Naciones Unidas contra la falsificación y el tráfico ilícitos de armas de fuego.

[100] Fuente: Europol.

[101] Europol, Centro Europeo de la Lucha contra el Tráfico Ilícito de Migrantes (EMSC), 4.º Informe anual.

[102] Evaluación de respuesta rápida de PNUMA-INTERPOL: The Rise of Environmental Crime (El aumento de los delitos medioambientales), de junio de 2016.

sostenible. Además de promover la acción de la UE, los Estados miembros y la comunidad internacional por incrementar los esfuerzos contra los delitos medioambientales[103], la Comisión está evaluando si la Directiva sobre delitos medioambientales[104] sigue ajustándose a sus objetivos. El **tráfico de bienes culturales**, en aumento, también se ha convertido en una de las actividades delictivas más lucrativas y es fuente de financiación del terrorismo y la delincuencia organizada. Deben estudiarse medidas para mejorar la trazabilidad en línea y fuera de línea de los bienes culturales en el mercado interior, la cooperación con los terceros países origen de los bienes culturales saqueados y el apoyo activo a las autoridades policiales y académicas.

A pesar de su gran complejidad, los **delitos económicos y financieros** afectan cada año a millones de ciudadanos y a miles de empresas en la UE. La lucha contra el fraude es crucial y requiere una actuación a nivel de la UE. Europol, junto con Eurojust, la Fiscalía Europea y la Oficina Europea de Lucha contra el Fraude, apoyan a los Estados miembros y a la UE en la protección de los mercados económicos y financieros y del dinero de los contribuyentes de la UE. La Fiscalía Europea será plenamente operativa a finales de 2020 e investigará, perseguirá y enjuiciará delitos contra el presupuesto de la UE, como el fraude, la corrupción y el blanqueo de dinero. También abordará el fraude transfronterizo del IVA que cuesta a los contribuyentes al menos 50 000 millones de euros al año

La Comisión también apoyará el desarrollo de conocimientos especializados y de un marco legislativo para riesgos emergentes del tipo de los criptoactivos y los nuevos sistemas de pago. En particular, la Comisión estudiará la respuesta a la aparición de criptoactivos, como el bitcóin, y al efecto que tendrán estas nuevas tecnologías en la forma de emitir, intercambiar, compartir y acceder a los activos financieros.

La Unión Europea debe tener tolerancia cero con respecto al dinero ilícito. Desde hace más de treinta años, la UE ha desarrollado un sólido marco normativo para la prevención y la lucha contra el **blanqueo de capitales** y la financiación del terrorismo, respetando plenamente la necesidad de proteger los datos personales. No obstante, existe un consenso cada vez mayor en torno a la idea de que la aplicación del marco actual debe mejorar considerablemente. Hay que abordar las grandes divergencias en las modalidades de aplicación y las graves deficiencias en la aplicación de las normas. Como se detalla en el plan de acción de mayo de 2020[105], se está trabajando en la evaluación de opciones para mejorar el marco de la UE para la lucha contra el blanqueo de capitales y la financiación del terrorismo. Entre las cuestiones que deben explorarse cabe citar la interconexión de los registros nacionales centralizados de cuentas bancarias, lo que podría acelerar considerablemente el acceso a la información financiera para las unidades de información financiera y las autoridades competentes.

Los **beneficios de los grupos delictivos organizados** en la UE se estiman en 110 000 millones de euros anuales. La respuesta actual a esta situación incluye una legislación armonizada en materia de decomiso y recuperación de activos[106] para mejorar el embargo preventivo y el decomiso de activos de origen delictivo en la UE y facilitar la confianza mutua y la cooperación transfronteriza efectiva entre los Estados miembros. Sin embargo,

[103] Véase el Pacto Verde Europeo, COM(2019) 640 final.
[104] Directiva 2008/99/CE relativa a la protección del medio ambiente mediante el Derecho penal.
[105] Plan de acción para la prevención del blanqueo de capitales y la financiación del terrorismo, COM(2020) 2800.
[106] La legislación de la UE exige que todos los Estados miembros cuenten con un organismo de recuperación de activos.

solo se confisca alrededor del 1 % de estos beneficios[107], lo que permite a los grupos delictivos organizados invertir en la expansión de sus actividades delictivas e infiltrarse en la economía legal. Las pymes, que tienen dificultades para acceder al crédito, son, en particular, un objetivo clave para el blanqueo de dinero. La Comisión analizará la aplicación de la legislación[108] y la posible necesidad de normas comunes adicionales, incluido el decomiso no basado en condena.

También podría dotarse a los organismos de recuperación de activos[109], agentes clave en el proceso de recuperación de activos, de mejores herramientas para identificar y localizar de forma más rápida los activos en toda la UE con el fin de aumentar el número de decomisos.

Existe una estrecha relación entre la delincuencia organizada y la **corrupción**. Se ha estimado que, por sí sola, la corrupción cuesta a la economía de la UE aproximadamente 120 000 millones de euros al año[110]. La prevención y la lucha contra la corrupción seguirán siendo objeto de un seguimiento periódico por lo que se refiere a la situación del Estado de Derecho, así como en el marco del Semestre Europeo. El Semestre Europeo ha evaluado los ámbitos en los que se plantean retos de lucha contra la corrupción, como la contratación pública, la administración pública, el entorno empresarial o la asistencia sanitaria. El nuevo informe anual sobre el Estado de Derecho de la Comisión cubrirá la lucha contra la corrupción y permitirá un diálogo preventivo con las autoridades nacionales y las partes interesadas a nivel nacional y de la UE. Las organizaciones de la sociedad civil también pueden desempeñar un papel clave a la hora de estimular la actuación de las autoridades públicas en la prevención y la lucha contra la delincuencia organizada y la corrupción, por lo que sería útil reunir a estos grupos en un foro común. Debido a su carácter transfronterizo, otra factor clave es la cooperación en materia de delincuencia organizada y corrupción con las regiones vecinas de la UE y la asistencia a las mismas.

Acciones clave
• Agenda de lucha contra el terrorismo de la UE, incluidas las medidas renovadas de lucha contra la radicalización en la UE • Nueva cooperación con terceros países y organizaciones internacionales clave en la lucha contra el terrorismo • Agenda para la lucha contra la delincuencia organizada, incluida la trata de seres humanos • Agenda y plan de acción de la UE en materia de lucha contra la droga 2021-2025 • Evaluación del Observatorio europeo de la droga y las toxicomanías • Plan de acción de la UE sobre el tráfico de armas de fuego 2020-2025 • Revisión de la legislación relativa al embargo preventivo y decomiso y a los organismos de recuperación de activos

[107] Informe «Recuperación de activos y decomiso: Garantizar que el delito no resulte provechoso», COM(2020) 0217.

[108] Directiva 2014/42/UE sobre el embargo y el decomiso de los instrumentos y del producto del delito en la Unión Europea.

[109] Decisión 2007/845/JAI del Consejo sobre cooperación entre los organismos de recuperación de activos de los Estados miembros en el ámbito del seguimiento y la identificación de productos del delito o de otros bienes relacionados con el delito.

[110] La estimación de los costes económicos totales de la corrupción es difícil, aunque organismos como la Cámara de Comercio Internacional, Transparencia Internacional, el Pacto Mundial de las Naciones Unidas y el Foro Económico Mundial han llevado a cabo trabajos que sugieren que la corrupción representa el 5 % del PIB mundial.

- Evaluación de la Directiva relativa a la protección del medio ambiente mediante el Derecho penal
- Plan de acción de la UE contra el tráfico ilícito de migrantes 2021-2025

4. Un ecosistema de seguridad europeo sólido

El logro de una Unión de la Seguridad genuina y efectiva debe ser el objetivo del esfuerzo común de todos los sectores de la sociedad. Los gobiernos, los cuerpos y fuerzas de seguridad, el sector privado, el educativo y los propios ciudadanos deben estar comprometidos, equipados, y adecuadamente conectados para establecer las capacidades de preparación y resiliencia de todas las víctimas, en particular las más vulnerables, y los testigos.

Todas las políticas precisan de una dimensión de seguridad y la UE puede contribuir a todos los niveles. En el hogar, la violencia doméstica es uno de los riesgos más graves para la seguridad. En la UE, el 22 % de las mujeres ha padecido un trato violento de su pareja[111]. La adhesión de la UE al Convenio de Estambul sobre prevención y lucha contra la violencia contra las mujeres y la violencia doméstica sigue siendo una prioridad clave. En caso de que las negociaciones sigan estando bloqueadas, la Comisión adoptará otras medidas para alcanzar los mismos objetivos que el Convenio, incluida la propuesta de añadir la violencia contra las mujeres a la lista de delitos definidos en el Tratado.

Cooperación e intercambio de información

Una de las contribuciones más críticas de la UE para proteger a los ciudadanos es ayudar a los responsables de la seguridad a trabajar conjuntamente. La cooperación y el intercambio de información son las herramientas más eficaces para luchar contra la delincuencia y el terrorismo y avanzar en pos de la justicia. Pero, para ser eficaces, han de ser específicos y oportunos. Para ser fiables, deben utilizarse con salvaguardias y controles comunes.

Se han creado una serie de instrumentos y estrategias sectoriales específicos de la UE[112] para seguir desarrollando la **cooperación policial operativa** entre los Estados miembros. Uno de los principales instrumentos de la UE en favor de la cooperación policial entre Estados miembros es el Sistema de Información de Schengen, utilizado para intercambiar datos sobre personas buscadas y desaparecidas en tiempo real. Los resultados se han hecho patentes por lo que respecta a la detención de delincuentes, la incautación de drogas y el rescate de víctimas potenciales[113]. Aun así, el nivel de cooperación podría mejorarse mediante la racionalización y la mejora de los instrumentos disponibles. La mayor parte del entramado legal de la UE que sustenta la cooperación policial operativa fue concebido hace 30 años. Una red compleja de acuerdos bilaterales entre Estados miembros, muchos de los cuales han quedado obsoletos o son raramente invocados, que amenaza con fragmentarse. En los países más pequeños o sin litoral, los agentes de las fuerzas policiales que trabajan en misiones transfronterizas deben cumplir cuando llevan a cabo acciones operativas hasta siete conjuntos de normas distintos en algunos casos. El resultado es que algunas operaciones, como las persecuciones en caliente de sospechosos a través de fronteras interiores, sencillamente no se producen. En el actual marco de la UE, la cooperación operativa tampoco tiene en cuenta nuevas tecnologías como los drones.

[111] Una Unión de la igualdad: Estrategia para la Igualdad de Género 2020-2025, COM(2020) 152.

[112] Como el Plan de Acción de la Estrategia de Seguridad Marítima de la UE, que dio lugar a importantes logros con la cooperación en las tareas de guardacostas entre las agencias de la UE pertinentes.

[113] Lucha de la UE contra la delincuencia organizada en 2019 (Consejo, 2020).

La eficacia operativa puede sustentarse en una cooperación policial específica, que también puede ayudar a proporcionar un soporte clave a otros objetivos políticos, como la aportación de la seguridad a la nueva evaluación de la inversión extranjera directa. En este sentido, la Comisión estudiará cual puede ser la contribución de un Código de Cooperación Policial. Las autoridades policiales de los Estados miembros han recurrido cada vez más a la ayuda y los conocimientos especializados disponibles a escala de la UE, mientras que el INTCEN ha desempeñado un papel clave en la promoción del intercambio de inteligencia estratégica entre los servicios de inteligencia y seguridad de los Estados miembros, proporcionando a las instituciones de la UE una conciencia situacional basada en la inteligencia[114]. **Europol** también puede desempeñar un papel clave a la hora de ampliar su cooperación con terceros países para luchar contra la delincuencia y el terrorismo de forma coherente con otras políticas e instrumentos exteriores de la UE. Sin embargo, Europol se enfrenta hoy a una serie de limitaciones graves, en particular en lo que se refiere al intercambio directo de datos personales con las partes privadas, lo que le impide ayudar de forma eficaz a los Estados miembros en la lucha contra el terrorismo y la delincuencia. En la actualidad se está evaluando el mandato de Europol para ver cómo debe mejorarse a fin de garantizar que la Agencia pueda desempeñar plenamente sus funciones. En este contexto, las autoridades pertinentes a nivel de la UE (como la OLAF, Europol, Eurojust y la Fiscalía Europea) también deben cooperar más estrechamente y mejorar el intercambio de información.

Otra conexión clave es el desarrollo de **Eurojust** para maximizar la sinergia entre la cooperación policial y judicial. La UE también se beneficiaría de una mayor coherencia estratégica: **EMPACT**[115], el ciclo político de la UE para la delincuencia organizada y las formas graves de delincuencia organizada, proporciona a las autoridades una metodología criminal basada en inteligencia para abordar conjuntamente las amenazas delictivas más importantes que afectan a la UE. Ha dado importantes resultados operativos[116] en la pasada década. Contando con la experiencia de los profesionales, es preciso racionalizar y simplificar el mecanismo existente para abordar mejor las amenazas más urgentes y cambiantes de cara al nuevo ciclo político del periodo 2022-2025.

La **información** oportuna y pertinente es fundamental para el trabajo diario de persecución de la delincuencia. A pesar del desarrollo de nuevas bases de datos de la UE en materia de seguridad y gestión de fronteras, mucha información se encuentra todavía en bases de datos nacionales o se intercambia al margen de estas herramientas. El resultado es una carga de trabajo adicional importante, retrasos y un aumento del riesgo de pérdida de información clave. Unos procesos mejores, más rápidos y simplificados, con la participación de todos los colectivos involucrados en el sector de la seguridad, aportarían mejores resultados. Para que el intercambio de información logre su potencial a la hora de lograr la persecución efectiva de los delitos, son esenciales las herramientas adecuadas dotadas de las salvaguardias necesarias para que la puesta en común de datos respete las leyes de protección de datos y los derechos fundamentales. A la luz de la evolución tecnológica, forense y de protección de datos, y de los cambios en las necesidades operativas, la UE podría considerar la necesidad de modernizar instrumentos como las **Decisiones de Prüm de 2008**, estableciendo un intercambio automatizado de datos de ADN, huellas dactilares y registro de vehículos a fin de permitir el intercambio automático de categorías de datos adicionales que ya están

[114] El INTCEN sirve de pasarela para los servicios de inteligencia y seguridad de los Estados miembros con el fin de proporcionar a la UE una conciencia situacional basada en los servicios de inteligencia.

[115] EMPACT, European Multidisciplinary Platform Against Criminal Threats (Plataforma multidisciplinar europea contra las amenazas delictivas).

[116] https://data.consilium.europa.eu/doc/document/ST-7623-2020-INIT/en/pdf.

disponibles en las bases de datos penales o de otro tipo de los Estados miembros a efectos de investigaciones penales. Además, la Comisión estudiará la posibilidad de intercambiar ficheros policiales para ayudar a identificar si existe un fichero policial de una persona en otro Estado miembro y facilitar el acceso al mismo una vez identificado, con todas las salvaguardias necesarias.

La **información sobre los viajeros** ha contribuido a mejorar los controles fronterizos, a reducir la migración irregular e identificar a las personas que constituyen un riesgo para la seguridad. Los datos de información anticipada de los pasajeros son los datos biográficos de cada pasajero recogidos por las compañías aéreas durante la facturación y enviados previamente a las autoridades de control fronterizo en el lugar de destino. La revisión del marco jurídico[117] podría permitir un uso más eficaz de la información, al tiempo que se garantiza el cumplimiento de la legislación en materia de protección de datos y se facilita el flujo de pasajeros. Los registros de nombres de pasajeros (PNR) son los datos facilitados por los pasajeros a la hora de reservar su vuelo. La aplicación de la Directiva PNR[118] es clave, y la Comisión seguirá apoyando y haciendo cumplir sus disposiciones. Además, como acción a medio plazo, la Comisión pondrá en marcha una revisión del enfoque actual sobre **la transferencia de datos PNR a terceros países**.

La **cooperación judicial** es un complemento necesario de los esfuerzos policiales para luchar contra la delincuencia transfronteriza. La cooperación judicial ha experimentado un cambio más profundo en los últimos veinte años. Organismos como la **Fiscalía Europea** y **Eurojust** necesitan disponer de medios para funcionar plenamente o reforzarse También podría mejorarse la cooperación entre profesionales de la justicia, a través de medidas adicionales sobre el reconocimiento mutuo de las decisiones judiciales, la formación judicial y el intercambio de información. El objetivo debe ser aumentar la confianza mutua entre los jueces y fiscales, que es fundamental para el buen desarrollo de los procedimientos transfronterizos. El uso de **tecnologías digitales** también puede mejorar la eficiencia de nuestros sistemas judiciales. Se está creando un nuevo sistema de intercambio digital para transmitir órdenes europeas de investigación, solicitudes de asistencia judicial mutua y comunicaciones conexas entre los Estados miembros, con el apoyo de Eurojust. La Comisión trabajará con los Estados miembros para acelerar el despliegue de los sistemas informáticos necesarios a nivel nacional.

La cooperación internacional también es clave para una cooperación policial y judicial eficaz. Los acuerdos bilaterales con los principales socios desempeñan un papel clave a la hora de garantizar la información y los elementos de prueba de fuera de la UE. **Interpol**, una de las mayores organizaciones intergubernamentales de policía judicial, cumple un papel importante. La Comisión estudiará posibles vías para reforzar la cooperación con Interpol, incluido el posible acceso a sus bases de datos y el refuerzo de la cooperación operativa y estratégica. Las autoridades policiales de la UE también confían en países socios clave para detectar e investigar a delincuentes y terroristas. Podrían intensificarse las **asociaciones de seguridad entre la UE y terceros países** a fin de aumentar la cooperación para hacer frente a amenazas comunes como el terrorismo, la delincuencia organizada, la ciberdelincuencia, el abuso sexual de menores y la trata de seres humanos. Este enfoque se basaría en intereses

[117] Directiva 2004/82/CE del Consejo sobre la obligación de los transportistas de comunicar los datos de las personas transportadas

[118] Directiva (UE) 2016/681 relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave.

comunes en materia de seguridad y partiría de la cooperación y de los diálogos sobre seguridad establecidos.

Además de la información, el intercambio de conocimientos especializados puede tener un valor particular para aumentar el grado de preparación de las fuerzas policiales frente a las **amenazas no tradicionales**. Además de fomentar los intercambios de mejores prácticas, la Comisión estudiará un posible **mecanismo de coordinación a escala de la UE para las fuerzas policiales** en casos de fuerza mayor, como pandemias. La pandemia también ha demostrado que la policía de proximidad digital, acompañada de marcos jurídicos para facilitar los servicios policiales en línea, será fundamental en la lucha contra la delincuencia y el terrorismo. Las asociaciones entre la policía y las comunidades, tanto en línea como fuera de línea, pueden prevenir la delincuencia y mitigar el impacto de la delincuencia organizada, la radicalización y las actividades terroristas. La conexión de las soluciones policiales a escala local, regional, nacional y de la UE es un factor clave para el éxito de la Unión de la Seguridad en su conjunto.

La contribución de unas fronteras exteriores fuertes

La gestión moderna y eficaz de las fronteras exteriores tiene el doble beneficio de mantener la integridad de Schengen y garantizar la seguridad de nuestros ciudadanos. La participación de todos los agentes pertinentes para garantizar un máximo de seguridad en las fronteras puede tener un impacto real en la prevención de la delincuencia transfronteriza y el terrorismo. Las actividades operativas conjuntas de la Guardia Europea de Fronteras y Costas[119], recientemente reforzadas, contribuyen a la prevención y la detección de la delincuencia transfronteriza en las **fronteras exteriores** e incluso fuera de la UE. Las actividades aduaneras de detección de los riesgos para la seguridad de todas las mercancías antes de su llegada a la UE y de control de las mercancías que llegan son cruciales en la lucha contra la delincuencia transfronteriza y el terrorismo. El próximo plan de acción sobre la Unión Aduanera anunciará acciones para reforzar la gestión de riesgos y mejorar la seguridad interior, en particular evaluando la viabilidad de un enlace entre los sistemas de información pertinentes para el análisis de riesgos en materia de seguridad.

En mayo de 2019 se adoptó el marco de **interoperabilidad entre los sistemas de información de la UE** en el ámbito de la justicia y los asuntos de interior. Esta nueva arquitectura pretende mejorar la eficiencia y la eficacia de los sistemas de información nuevos o perfeccionados[120]. Permitirá disponer de una información más rápida y sistemática a los agentes policiales, los guardias de fronteras y los funcionarios de los servicios de migración. Contribuirá a la correcta identificación y a combatir la usurpación de identidad. Para lograr todo ello es prioritario conseguir una interoperabilidad efectiva, tanto a nivel político como técnico. La estrecha cooperación entre las agencias de la UE y todos los Estados miembros será fundamental para alcanzar el objetivo de la plena interoperabilidad para 2023.

El **fraude en los documentos de viaje** se considera uno de los delitos más frecuentes. Facilita el movimiento clandestino de delincuentes y terroristas, y desempeña un papel clave

[119] Compuesta de la Agencia Europea de la Guardia de Fronteras y Costas (Frontex) y las autoridades de guardia de fronteras de los Estados miembros y de la guardia de costas de los Estados miembros.

[120] El Sistema de Entradas y Salidas (SES), el Sistema Europeo de Información y Autorización de Viajes (SEIAV), el Sistema Europeo de Información de Antecedentes Penales (ECRIS-TCN) ampliado, el Sistema de Información de Schengen, el Sistema de Información de Visados y el futuro Eurodac.

en la trata de seres humanos y el tráfico de drogas[121]. La Comisión estudiará cómo ampliar los trabajos existentes sobre las normas de seguridad de los documentos de viaje y de residencia de la UE, en particular a través de la digitalización. A partir de agosto de 2021, los Estados miembros empezarán a expedir documentos de identidad y de residencia con arreglo a normas de seguridad armonizadas, que incorporarán un chip con identificadores biométricos verificables por parte de todas las autoridades fronterizas de la UE. La Comisión supervisará la aplicación de estas nuevas normas y la sustitución gradual de los documentos actualmente en circulación.

Reforzar la investigación y la innovación en materia de seguridad

El trabajo para garantizar la ciberseguridad y la lucha contra la delincuencia organizada, la ciberdelincuencia y el terrorismo depende en gran medida del desarrollo de herramientas para el futuro: ayudar a crear nuevas tecnologías más seguras, abordar los retos que planteen las tecnologías y apoyar el trabajo de los cuerpos y fuerzas de seguridad. Esto, a su vez, depende de socios e industrias privados.

La innovación debe considerarse una herramienta estratégica para contrarrestar las amenazas actuales y anticiparse a los riesgos y oportunidades futuros. Las tecnologías innovadoras pueden aportar nuevos instrumentos para ayudar a los cuerpos y fuerzas de seguridad y a otros agentes del ámbito de la seguridad. La inteligencia artificial y el análisis de macrodatos podrían aprovechar la informática de alto rendimiento para ofrecer una mejor detección y un análisis rápido y exhaustivo[122]. Una condición previa clave para desarrollar tecnologías fiables es contar con conjuntos de datos de alta calidad, de los que las autoridades competentes dispongan para desarrollar, probar y validar algoritmos[123]. De manera más general, el riesgo de dependencia tecnológica en la actualidad es alto: la UE es, por ejemplo, un importador neto de productos y servicios de ciberseguridad, con todo lo que ello implica para la economía y las infraestructuras críticas. Para garantizar el dominio de la tecnología y la continuidad del suministro incluso en caso de acontecimientos y crisis adversos, Europa necesita presencia y capacidad en las partes críticas de las cadenas de valor pertinentes.

La **investigación, la innovación y el desarrollo tecnológico** de la UE ofrecen la oportunidad de tener en cuenta la dimensión de la seguridad a medida que se desarrollan estas tecnologías y su aplicación. La próxima generación de propuestas de financiación de la UE puede actuar como un importante estímulo[124]. Las iniciativas sobre los espacios de datos europeos y las infraestructuras de computación en la nube han tenido en cuenta el factor de la seguridad desde el principio. El Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación[125] tienen por objetivo establecer una estructura eficaz y eficiente para poner en común y compartir las capacidades y los resultados de la investigación en materia de ciberseguridad.

[121] La relación entre el fraude documental y la trata de seres humanos se establece en el segundo informe sobre los progresos realizados en la lucha contra la trata de seres humanos, [COM(2018) 777], en el documento adjunto [SWD(2018) 473], y en el Informe de situación sobre la trata de seres humanos en la UE de 2016, de Europol.

[122] Esto debería basarse en la estrategia de la Comisión sobre inteligencia artificial.

[123] Estrategia europea en materia de datos, COM(2020) 66 final.

[124] Todas las propuestas de la Comisión para Horizonte Europa, el Fondo de Seguridad Interior, el Fondo para la Gestión Integrada de las Fronteras, el Programa InvestEU, el Fondo Europeo de Desarrollo Regional y el Programa Europa Digital apoyarán el desarrollo y el despliegue de tecnologías y soluciones innovadoras en materia de seguridad a lo largo de la cadena de valor.

[125] Propuesta de Reglamento, de 12 de septiembre de 2018, por el que se establecen el Centro Europeo de Competencia Industrial, Tecnológica y de Investigación en Ciberseguridad y la Red de Centros Nacionales de Coordinación [COM(2018) 630].

El programa espacial de la UE presta servicios de apoyo a la seguridad de la UE, de sus Estados miembros y de los particulares[126].

Con más de 600 proyectos puestos en marcha por un valor global de cerca de 3 000 millones de euros desde 2007, la investigación en materia de seguridad financiada por la UE es un instrumento clave para impulsar la tecnología y los conocimientos aplicables a las soluciones de seguridad. En el marco de la revisión del mandato de Europol, la Comisión estudiará la creación de un **centro europeo de innovación para la seguridad interior**[127] que tenga por objeto aportar soluciones conjuntas a retos y oportunidades en materia de seguridad comunes que los Estados miembros no podrían aprovechar por sí solos. La cooperación es fundamental para orientar la inversión de forma que tenga la máxima efectividad y para desarrollar tecnologías innovadoras que ofrezcan beneficios tanto económicos como en materia de seguridad.

Capacidades y sensibilización

La sensibilización respecto de las cuestiones de seguridad y la adquisición de las capacidades necesarias para hacer frente a las amenazas potenciales son esenciales para construir una sociedad más resiliente y mejorar la preparación de empresas, administraciones y ciudadanos. Los retos a los que se han enfrentado la infraestructura informática y los sistemas electrónicos han puesto de manifiesto la necesidad de mejorar nuestra capacidad humana para la preparación y respuesta en materia de ciberseguridad. La pandemia también ha puesto de manifiesto la importancia de la digitalización en todos los ámbitos de la economía y la sociedad de la UE.

Basta con un **conocimiento básico de las amenazas para la seguridad** y de la manera de combatirlas para conseguir un impacto real en el grado de resiliencia de la sociedad. La concienciación sobre los riesgos de la ciberdelincuencia y la necesidad de protegerse ante ellos pueden añadirse a la protección de los proveedores de servicios frente a los ciberataques. La información sobre los peligros y riesgos del tráfico de drogas puede obstaculizar las actividades de los delincuentes. La UE puede estimular la difusión de las mejores prácticas, por ejemplo a través de la red de Centros de Seguridad en Internet[128], y garantizar que dichos objetivos se tengan en cuenta en sus propios programas.

El futuro Plan de Acción de Educación Digital debe incluir medidas específicas para dotar de competencias en materia de seguridad informática a toda la población. La Agenda de Capacidades[129] recientemente adoptada apoya el desarrollo de capacidades a lo largo de la vida de una persona. Incluye acciones específicas para aumentar el número de titulados en ciencia, tecnología, ingeniería, artes y matemáticas necesarios en ámbitos punteros, como la ciberseguridad. Otras acciones, financiadas por el programa Europa Digital, permitirán a los profesionales adaptarse al ritmo de evolución de las amenazas para la seguridad al tiempo que cubren las necesidades del mercado laboral de la UE en este ámbito. El impacto global consistirá en permitir a las personas adquirir competencias para hacer frente a las amenazas

[126] Por ejemplo, Copernicus presta servicios que permiten la vigilancia de las fronteras exteriores y la vigilancia marítima de la UE, lo que ayuda a luchar contra la piratería y el tráfico ilícito de migrantes, así como a apoyar infraestructuras críticas. Una vez que esté plenamente operativo, será clave para las misiones y operaciones civiles y militares.

[127] Esto se aplica también a AEGFC/Frontex, CEPOL, eu-LISA y el Centro Común de Investigación.

[128] Véase www.betterinternetforkids.eu: el portal central y los Centros de Seguridad en Internet nacionales se financian actualmente a través del Mecanismo «Conectar Europa» (MCE)/Telecom; para la futura financiación futura se ha propuesto en el programa Europa Digital.

[129] Agenda de Capacidades Europea para la competitividad sostenible, la equidad social y la resiliencia [COM(202) 274 final].

para la seguridad y a las empresas encontrar los profesionales que necesiten para ello. El próximo Espacio Europeo de Investigación y el Espacio Europeo de Educación también promoverán carreras en los ámbitos de la ciencia, la tecnología, la ingeniería, las artes y las matemáticas.

También es importante que las **víctimas** puedan valerse de los derechos que les asisten, para lo que deben recibir la asistencia y el apoyo necesarios en función de sus circunstancias específicas. Por lo que se refiere a las minorías y a las víctimas más vulnerables, como niños o mujeres víctimas de la trata con fines de explotación sexual o expuestos a la violencia doméstica[130], se hacen necesarias medidas especiales.

La mejora de las competencias es especialmente importante por lo que se refiere a las **capacidades de las fuerzas y cuerpos de seguridad**. Las nuevas amenazas tecnológicas actuales exigen invertir más en la formación de personal de las fuerzas y cuerpos de seguridad en la fase más temprana posible y a lo largo de toda su carrera profesional. CEPOL es un socio esencial para ayudar a los Estados miembros en esta tarea. La formación de las fuerzas y cuerpos de seguridad sobre el racismo, la xenofobia y los derechos de los ciudadanos en general debe ser componente esencial de la cultura de la seguridad de la UE.. Los sistemas judiciales nacionales y los profesionales de la justicia también deben estar equipados para adaptarse y responder a desafíos sin precedentes. La formación es esencial para que las autoridades sobre el terreno aprovechen estas herramientas en una situación de servicio. Además, deben realizarse todos los esfuerzos necesarios para reforzar la integración de la perspectiva de género y reforzar la participación de las mujeres en los cuerpos y fuerzas de seguridad.

Acciones clave
• Reforzar el mandato de Europol • Explorar un «Código de Cooperación Policial» y una coordinación policial en tiempos de crisis a escala de la UE • Reforzar Eurojust para crear un enlace entre las autoridades judiciales y los cuerpos y fuerzas de seguridad • Revisar la Directiva relativa a la información anticipada sobre los pasajeros • Elaborar una Comunicación sobre la dimensión exterior de los registros de nombres de los pasajeros • Reforzar la cooperación entre la UE e Interpol • Establecer un marco para negociar la puesta en común de información con terceros países clave • Mejorar las normas de seguridad aplicables a los documentos de viaje • Estudiar la posibilidad de crear un centro europeo de innovación para la seguridad interior

V. Conclusiones

En un mundo cada vez más turbulento, la Unión Europea sigue siendo ampliamente considerada como uno de los lugares más seguros y mejor protegidos. No obstante, esta situación no debe darse por descontada.

[130] Véase la estrategia para la igualdad de género [COM(2020) 152]; la estrategia sobre derechos de las víctimas [COM(2020) 258]; y la estrategia europea en favor de una Internet más adecuada para los niños [COM(2012) 196].

La nueva estrategia de la Unión de la Seguridad sienta las bases de un ecosistema de seguridad que abarca a la sociedad europea en su conjunto. Se afianza sobre la certeza de que la seguridad es responsabilidad compartida. La seguridad afecta a todos. Todos los organismos públicos, las empresas, las organizaciones sociales, las instituciones y los ciudadanos deben asumir sus propias responsabilidades para aumentar la seguridad de nuestras sociedades.

Las cuestiones de seguridad deben ahora verse desde una perspectiva mucho más amplia que en el pasado. Hay que superar falsas distinciones entre la seguridad física y la digital. La Estrategia de la Unión de la Seguridad de la UE reúne toda la gama de necesidades en materia de seguridad y se centra en los ámbitos más críticos para la seguridad de la UE de cara a los próximos años. Asimismo tiene en cuenta que las amenazas para la seguridad no respetan las fronteras geográficas y reconoce el creciente vínculo entre la seguridad interior y exterior[131]. En este contexto, será importante que la UE coopere con los socios internacionales para proteger a todos los ciudadanos de la UE y mantenga una estrecha coordinación con la acción exterior de la UE para la aplicación de esta Estrategia.

Nuestra seguridad no es independiente de nuestros valores fundamentales. Todas las acciones e iniciativas propuestas en esta estrategia respetarán plenamente los derechos fundamentales y nuestros valores europeos. Estos son la base de nuestro estilo de vida europeo y deben seguir constituyendo la columna vertebral de todo nuestro trabajo.

Por último, la Comisión sigue siendo plenamente consciente de que el éxito de una política o acción se mide por el éxito de su aplicación. Por consiguiente, es necesario insistir una y otra vez en la aplicación y ejecución correctas de la legislación actual y futura. Para ello se realizará un seguimiento a través de informes periódicos de la Unión de la Seguridad y la Comisión mantendrá al Parlamento Europeo, el Consejo y las partes interesadas plenamente informados e implicados en todas las acciones pertinentes. Además, la Comisión está dispuesta a organizar debates conjuntos con las instituciones sobre la Estrategia de la Unión de la Seguridad con el fin de hacer balance de los avances conseguidos y examinar los retos futuros.

La Comisión invita al Parlamento Europeo y al Consejo a apoyar esta Estrategia de la Unión de la Seguridad como fundamento de la cooperación y la acción conjunta durante los próximos cinco años.

[131] Véase la EU Global Strategy (Estrategia Global de la UE)