



Bruselas, 18.10.2017  
COM(2017) 608 final

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

**Undécimo informe de evolución hacia una Unión de la Seguridad genuina y efectiva**

## I. INTRODUCCIÓN

Este es el undécimo informe mensual sobre los progresos realizados en la construcción de una Unión de la Seguridad genuina y efectiva, en el que se describen los avances en dos grandes pilares: la lucha contra el terrorismo, la delincuencia organizada y los medios que los sustentan, por un lado, y el refuerzo de nuestros mecanismos de defensa y el aumento de la resiliencia frente a esas amenazas, por otro.

En el Discurso sobre el Estado de la Unión<sup>1</sup>, el presidente Juncker subrayó que, partiendo de los auténticos progresos alcanzados en los tres últimos años, la Unión Europea debía mostrarse más enérgica en su lucha contra el terrorismo. Conforme a lo anunciado en la carta de intenciones<sup>2</sup> al Parlamento Europeo y a la Presidencia del Consejo y en la Hoja de ruta adjunta hacia una Unión más unida, más fuerte y más democrática, la Comisión presenta en este informe un **paquete de medidas antiterroristas** que habrán de aplicarse en los próximos dieciséis meses. Estas medidas operativas ayudarán a los Estados miembros a reparar las importantes vulnerabilidades que los recientes atentados terroristas han descubierto y supondrán una verdadera diferencia en cuanto al aumento de la seguridad. De ese modo, contribuirán a configurar una Unión de la Seguridad donde no quede resquicio alguno que los terroristas puedan aprovechar para cometer atrocidades. Junto a estas medidas prácticas a corto plazo, la Comisión está trabajando en la creación de una futura Unidad de Inteligencia Europea, conforme a lo anunciado por el presidente Juncker en su visión de la Unión Europea para 2025.

El paquete antiterrorista incluye:

- medidas para ayudar a los Estados miembros a **proteger los espacios públicos** (capítulo II), entre las que se incluye un Plan de acción para contribuir a la protección de los espacios públicos y un Plan de acción para mejorar la preparación ante los riesgos de seguridad químicos, biológicos, radiológicos y nucleares;
- medidas para **cortar el acceso a los medios empleados por los terroristas** para preparar y perpetrar los atentados, como las **sustancias peligrosas** o la **financiación del terrorismo** (capítulo III), entre las que se incluyen una Recomendación sobre las disposiciones inmediatas para impedir el uso indebido de precursores de explosivos y medidas de apoyo a las autoridades policiales y judiciales cuando se enfrenten al **uso de cifrado** en sus investigaciones penales;
- las próximas etapas de la **lucha contra la radicalización** (capítulo IV);
- los próximos pasos para reforzar la **dimensión exterior** de la lucha contra el terrorismo (capítulo V), incluidas las propuestas de Decisiones del Consejo sobre la celebración, en nombre de la UE, del Convenio del Consejo de Europa para la prevención del terrorismo y su Protocolo adicional, y una Recomendación al Consejo por la que se autoriza la apertura de negociaciones con Canadá para la revisión del Acuerdo sobre el registro de nombres de los pasajeros.

## II. MEDIDAS DE AUMENTO DE LA PROTECCIÓN Y LA RESILIENCIA FRENTE AL TERRORISMO

### 1. *Mejor protección de los espacios públicos*

<sup>1</sup> [http://europa.eu/rapid/press-release\\_SPEECH-17-3165\\_es.htm](http://europa.eu/rapid/press-release_SPEECH-17-3165_es.htm).

<sup>2</sup> [https://ec.europa.eu/commission/sites/beta-political/files/letter-of-intent-2017\\_es.pdf](https://ec.europa.eu/commission/sites/beta-political/files/letter-of-intent-2017_es.pdf).

Tanto en la actividad de propaganda como en la selección de objetivos, el punto de mira de los terroristas está desplazándose hacia los espacios públicos, como las zonas peatonales, los puntos turísticos, los nudos de transporte, los centros comerciales, las salas de concierto y las plazas públicas, lugares en los que se perpetraron los atentados de Barcelona, Berlín, Bruselas, Londres, Manchester, Niza, París y Estocolmo, por ejemplo. El denominador común de estos «blancos fáciles» es su carácter abierto y público, con una alta concentración de personas, que los hace intrínsecamente vulnerables.

Podemos hacer más por reducir la vulnerabilidad de estos espacios, detectando las amenazas en una fase más precoz y aumentando nuestra resiliencia. Con ese fin, la Comisión, a través de su **Plan de acción para contribuir a la protección de los espacios públicos**<sup>3</sup>, presentado junto con el presente informe, ha expuesto una serie de medidas con las que pretende ayudar a las autoridades nacionales, regionales y locales a reforzar la protección física contra las amenazas terroristas. Si bien es cierto que el «riesgo cero» no existe, los objetivos del Plan de acción son ayudar a los Estados miembros a detectar las amenazas, reducir la vulnerabilidad de los espacios públicos, mitigar las consecuencias de los posibles atentados terroristas y mejorar la cooperación.

La ayuda que la UE puede aportar a la protección de los espacios públicos es doble: en primer lugar, puede fomentar el **intercambio de las mejores prácticas entre los distintos países, destinando fondos a tal fin**. Esa iniciativa incluye, por ejemplo, medidas para promover y apoyar el desarrollo de barreras innovadoras y discretas que refuercen la seguridad de las ciudades sin desvirtuar su carácter abierto («protección desde el diseño»). Resuelta a sustentar las medidas del Plan de acción con el apoyo financiero adecuado, la Comisión ha publicado hoy una convocatoria de propuestas a través del Fondo de Seguridad Interior - Policía por un importe total de 18,5 millones EUR. Esta financiación a corto plazo se complementará en 2018 con la correspondiente a las Acciones Urbanas Innovadoras, enmarcadas en el Fondo Europeo de Desarrollo Regional, uno de cuyos temas clave será la seguridad, y cuya financiación total podrá llegar hasta 100 millones EUR. El 15 de septiembre de 2017 se abrió una consulta pública con el fin de recabar de las ciudades ideas sobre soluciones innovadoras en materia de seguridad. Sus resultados ayudarán a la Comisión a organizar las próximas convocatorias de propuestas en este ámbito.

En segundo lugar, la UE puede fomentar la **cooperación con un amplio abanico de interesados**, enfoque que se considera crucial para aumentar la protección de los espacios públicos. El intercambio de experiencias y la puesta en común de recursos deben estructurarse mejor. La Comisión abrirá un foro para comunicarse con los agentes del sector privado, como los centros comerciales, los organizadores de conciertos, los estadios deportivos y las empresas de alquiler de coches. Ese canal facilitará una toma de conciencia común de los actuales retos en materia de seguridad y fomentará asociaciones público-privadas destinadas a aumentar la protección. También las autoridades locales y regionales tienen un papel fundamental que desempeñar en la protección de los espacios públicos, por lo que deben estar asociadas a las actividades correspondientes que se realicen al nivel de la UE. La Comisión aumentará la implicación de estas partes interesadas y entablará un diálogo con las autoridades regionales y locales, como los alcaldes, para la puesta en común de información y

---

<sup>3</sup> COM(2017) 612 final (18.10.2017).

de las mejores prácticas a este respecto. Conforme a lo anunciado en la Declaración de Niza<sup>4</sup> de 29 de septiembre de 2017, la Comisión organizará el año próximo, junto con el Comité de las Regiones, una reunión de alto nivel con los alcaldes firmantes de dicha Declaración y otros representantes de las instancias locales y regionales, con miras a continuar el intercambio de las mejores prácticas sobre protección de espacios públicos.

La Comisión proseguirá asimismo su labor de protección y aumento de la resiliencia de la **infraestructura crítica**. La evaluación global de la política de seguridad de la UE<sup>5</sup> indicó también la necesidad de adaptar el Programa Europeo de Protección de Infraestructuras Críticas<sup>6</sup> a las amenazas emergentes. La Comisión ha iniciado una evaluación de la Directiva<sup>7</sup> sobre la identificación y designación de infraestructuras críticas europeas. En ella se tendrán en cuenta las enseñanzas extraídas y la evolución de la situación en los últimos años, como la adopción de la Directiva sobre seguridad de las redes y de la información<sup>8</sup>. Entre tanto, se ha reforzado el Programa Europeo de Protección de Infraestructuras Críticas, prestando atención a ciertos desafíos emergentes como las amenazas internas y las amenazas híbridas, y ampliando la vertiente exterior del programa mediante la cooperación con los países de la vecindad oriental y los Balcanes Occidentales.

Desde hace muchos años, el sector de los transportes ha sido tanto el blanco de los atentados terroristas como el medio utilizado para perpetrarlos (por ejemplo, el secuestro de aviones o el atropello con camiones). En respuesta a esa situación, es necesario evaluar en qué medida las normas de **seguridad del transporte** garantizan la seguridad sin menoscabo de la fluidez de las redes de transporte. Dado que el sector de la aviación está considerablemente más protegido, los atentados terroristas se han desplazado, de forma oportunista, hacia los espacios públicos. Entre ellos, el **transporte ferroviario** es un objetivo de alto riesgo debido a su infraestructura abierta por naturaleza. No existe en la actualidad ningún marco legislativo de la UE que proteja al transporte de pasajeros por ferrocarril del terrorismo y las formas de delincuencia graves. El 15 de junio de 2017, la Comisión emprendió, junto con los Estados miembros, una evaluación común de los riesgos del ferrocarril, y está preparando nuevas medidas para aumentar la seguridad de los viajeros ferroviarios. La Comisión está trabajando, además, en una guía práctica de seguridad, basada en las mejores soluciones, para el sector del **transporte comercial por carretera**. Su objetivo central será aumentar la seguridad de los camiones, mitigando el riesgo de intrusión no autorizada (incluidos el secuestro o el robo) en los vehículos para su utilización en un atentado terrorista por atropello. La guía práctica,

---

<sup>4</sup> La Declaración de Niza se aprobó en el congreso de alcaldes de la región euromediterránea celebrado en Niza el 29 de septiembre de 2017 y organizado a iniciativa del alcalde de esa ciudad, con la participación de la Comisión, con el fin de intercambiar las mejores prácticas de prevención de la radicalización y protección de espacios públicos entre las ciudades y las entidades locales y regionales. <http://www.nice.fr/uploads/media/default/0001/15/TERRORISME%20EUROPE%20Déclaration%20-%20der%20version.pdf>.

<sup>5</sup> Véase el noveno informe de situación relativo a una Unión de la Seguridad genuina y efectiva (COM(2017) 407 final de 26.7.2017) y el documento de trabajo de los servicios de la Comisión adjunto (SWD(2017) 278 final).

<sup>6</sup> El Programa Europeo de Protección de Infraestructuras Críticas establece el marco para las actividades de la UE destinadas a aumentar la protección de la infraestructura crítica en Europa, en todos los Estados miembros y en todos los sectores de actividad económica pertinentes. Uno de los pilares fundamentales de esta labor es la Directiva de 2008 sobre la identificación y designación de infraestructuras críticas europeas (Directiva 2008/114/CE de 8.12.2008).

<sup>7</sup> Directiva 2008/114/CE (8.12.2008).

<sup>8</sup> Directiva 2016/1148/CE (6.7.2016).

que estará disponible antes de que termine 2017, ofrecerá recomendaciones a los sectores nacionales de transporte por carretera. La Comisión proseguirá asimismo su labor de refuerzo de la **seguridad del transporte marítimo**, destinada en particular a aumentar la protección de las infraestructuras de transporte marítimo, entre las que se incluyen los puertos, las instalaciones portuarias, los buques portacontenedores y los buques de transporte de pasajeros como las embarcaciones de crucero y los transbordadores.

2. *Mejor preparación ante los riesgos de seguridad químicos, biológicos, radiológicos y nucleares*

Aunque la probabilidad de atentados con sustancias químicas, biológicas, radiológicas y nucleares (QBRN) en la UE sigue siendo baja, se detecta cierta evolución en esa amenaza en general. Existen indicios de que algunos delincuentes o grupos terroristas podrían tener la intención de adquirir material QBRN, además de la capacidad y los conocimientos necesarios para su utilización con fines terroristas. El potencial de los atentados de esta índole ocupa un lugar destacado en la propaganda terrorista. La evaluación global de la política de seguridad de la UE<sup>9</sup> indicó también la necesidad de intensificar la preparación frente a estas amenazas.

Para aumentar en los próximos años el nivel de preparación frente a las amenazas QBRN, la Comisión presenta, junto con el presente informe, un **Plan de acción para mejorar la preparación ante los riesgos de seguridad químicos, biológicos, radiológicos y nucleares**<sup>10</sup>. Incluye una amplia gama de medidas para mejorar la preparación, la resiliencia y la coordinación al nivel de la UE, mediante, por ejemplo, la creación de una red de seguridad frente al riesgo QBRN de la UE que reúna a todos los agentes implicados. La red se apoyará, entre otros medios, en un núcleo de conocimientos QBRN que albergará el Centro Europeo de Lucha contra el Terrorismo (CELT) en Europol. También es importante utilizar mejor los recursos existentes, por lo que el Plan de acción propone reforzar la preparación y la respuesta frente a la amenaza QBRN mediante formación teórica y práctica que se impartirá a todos los agentes de primera intervención (policía, protección civil, personal sanitario) y, cuando corresponda, a los interlocutores militares y del sector privado. La red se apoyará asimismo en las herramientas existentes a escala de la UE, como el Mecanismo de Protección Civil de la Unión (MPCU)<sup>11</sup> y la Agencia de la Unión Europea para la Formación Policial (CEPOL). Para ofrecer una mejor asistencia en caso de incidente QBRN grave, los Estados miembros deben seguir reforzando la Capacidad Europea de Respuesta a Emergencias (CERE) del MPCU. Se recomienda para ello a los Estados miembros que sigan asignando nuevos recursos al CERE.

La legislación de la UE en materia de **amenazas transfronterizas graves para la salud**<sup>12</sup> contempla medidas de preparación, vigilancia y coordinación de las respuestas ante las emergencias de orden sanitario en toda la UE. En este contexto, se mejorará la conexión del Sistema de Alerta Precoz y Respuesta de la UE con los demás sistemas de alerta de la UE ante amenazas biológicas, químicas, medioambientales y de origen desconocido. También se financian con cargo al Programa de salud ejercicios de preparación y respuesta frente a las

---

<sup>9</sup> Véase el noveno informe de situación relativo a una Unión de la Seguridad genuina y efectiva (COM(2017) 407 final de 26.7.2017) y el documento de trabajo de los servicios de la Comisión adjunto (SWD(2017) 278 final).

<sup>10</sup> COM(2017) 610 final (18.10.2017).

<sup>11</sup> Decisión 1313/2013/CE (17.12.2013).

<sup>12</sup> Decisión 1082/2013/UE (22.10.2013).

emergencias en toda la UE, así como acciones conjuntas para ayudar a los Estados miembros a reforzar los laboratorios, las campañas de vacunación y las capacidades básicas con arreglo al Reglamento Sanitario Internacional.

Todas las iniciativas se apoyarán en actividades específicas de investigación, financiación y cooperación con los interlocutores internacionales pertinentes.

### III. LUCHA CONTRA LOS MEDIOS EN LOS QUE SE SUSTENTA EL TERRORISMO

#### 1. *Financiación del terrorismo: acceso transfronterizo a la información financiera*

La información sobre las actividades financieras de los sospechosos puede proporcionar pistas cruciales para las investigaciones en la lucha antiterrorista. Por su fiabilidad y precisión, los datos financieros (incluidos los relativos a transacciones financieras) pueden ayudar a identificar a los terroristas, destapar vínculos con cómplices, determinar las actividades, la logística y los movimientos de los sospechosos y trazar las redes terroristas. Una rápida visión global de las actividades financieras de los sospechosos y sus cómplices puede aportar a las autoridades policiales y judiciales información esencial para prevenir atentados o reaccionar en el periodo inmediato a los mismos. El creciente fenómeno de los atentados burdos a pequeña escala presenta nuevos desafíos; los indicios de las conspiraciones y actuaciones previstas pueden resultar menos evidentes si su plazo de planificación es más corto. Las transacciones financieras asociadas con las tramas a pequeña escala pueden resultar poco sospechosas, de forma que las autoridades competentes no llegan a conocer esa información hasta después del atentado.

Conforme a lo anunciado en el Plan de acción de 2016 contra la financiación del terrorismo<sup>13</sup>, la **Comisión está estudiando la necesidad de adoptar medidas adicionales** para facilitar el acceso a la información financiera que obre en poder de otras jurisdicciones de la UE con miras a las investigaciones antiterroristas. En el Tercer informe de situación relativo a una Unión de la Seguridad genuina y efectiva, de diciembre de 2016<sup>14</sup>, la Comisión expuso su análisis inicial e indicó que proseguiría su evaluación, teniendo especialmente en cuenta las posibles repercusiones en los derechos fundamentales y, en particular, en el derecho a la protección de los datos personales. Desde entonces, la Comisión ha consultado a los interesados y analizado los mecanismos que permiten actualmente a las autoridades competentes acceder a la información pertinente, concretamente los datos financieros conservados en otros Estados miembros, los obstáculos que impiden hacerlo rápida y eficazmente y las posibles medidas para despejarlos.

Además de continuar esta evaluación, la Comisión sigue fomentando el **intercambio de buenas prácticas** en cuanto a las técnicas de investigación y los análisis de los métodos terroristas de recaudación y transferencia de fondos, para lo que aporta, entre otros recursos, ayuda financiera sobre la base de una convocatoria de propuestas por un importe de 2,5 millones EUR publicada hoy.

---

<sup>13</sup> COM(2016) 50 final (2.2.2016).

<sup>14</sup> COM(2016) 831 final (21.12.2016).

En este contexto, la Comisión está explorando, además, vías de **mejorar la cooperación entre las distintas unidades de inteligencia financiera**<sup>15</sup> creadas para prevenir, detectar y combatir eficazmente el blanqueo de capitales y la financiación del terrorismo. El informe sinóptico realizado en diciembre de 2016 por las unidades de inteligencia financiera y el correspondiente documento de trabajo de los servicios de la Comisión sobre la mejora de la cooperación entre dichas unidades<sup>16</sup> ponen de manifiesto una serie de limitaciones en las competencias nacionales de las mismas y proponen resolverlas mediante las intervenciones siguientes: i) aplicación de la 4.<sup>a</sup> Directiva contra el blanqueo de capitales<sup>17</sup>, incluidas sus modificaciones<sup>18</sup> actualmente en fase de negociación; ii) otras iniciativas llevadas a cabo por la plataforma de unidades de inteligencia financiera de la UE con el fin de mejorar la cooperación operativa, especialmente mediante orientación, normalización y soluciones de negocio aplicables a FIU.Net, y iii) medidas de regulación para solucionar otros problemas derivados de las divergencias entre el estatuto y las competencias de las distintas unidades de inteligencia financiera, en particular con el propósito de facilitar la coordinación y el intercambio de información, tanto entre las propias unidades de inteligencia financiera como entre estas y las autoridades policiales.

También se está trabajando para facilitar el **acceso a los datos financieros dentro de un Estado miembro**. Las modificaciones propuestas de la **4.<sup>a</sup> Directiva contra el blanqueo de capitales**<sup>19</sup>, actualmente en fase de negociación con los colegisladores, conduciría al establecimiento en todos los Estados miembros de registros centrales de cuentas bancarias accesibles para las unidades de inteligencia financiera y otras autoridades competentes responsables de la lucha contra el blanqueo de capitales y la financiación del terrorismo. Una vez creados en todos los Estados miembros, estos registros facilitarán la detección de datos relativos a las cuentas. Sobre esa base, la Comisión está preparando una iniciativa por la que **se ampliará el acceso de las autoridades policiales a dichos registros**<sup>20</sup>, con el fin de reforzar la capacidad de dichas autoridades para detectar con mayor rapidez la existencia de una cuenta bancaria.

Durante las consultas con los interesados se planteó también la cuestión de los **obstáculos a la obtención de datos sobre transacciones financieras conservados en otros Estados miembros**. En caso necesario, los Estados miembros pueden intercambiar información sobre cuentas bancarias en un plazo de ocho horas a través de los canales de cooperación policial<sup>21</sup>.

---

<sup>15</sup> Las unidades de inteligencia financiera se crearon en virtud de la Decisión 2000/642/JAI del Consejo (17.10.2000), desarrollándose su regulación en la Directiva 2015/849 (20.5.2015), relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo. Son unidades independientes y autónomas desde el punto de vista operativo, responsables de recibir y analizar las notificaciones de transacciones sospechosas y otra información, procedente de las entidades pertinentes, relacionada con el blanqueo de capitales, los delitos subyacentes o la financiación del terrorismo, y de poner en conocimiento de las autoridades competentes los resultados de sus análisis y toda información de interés adicional.

<sup>16</sup> SWD(2017)275 final (26.6.2017).

<sup>17</sup> Directiva 2015/849/CE (20.5.2015).

<sup>18</sup> COM(2016) 450 final (5.7.2016).

<sup>19</sup> COM(2016) 450 final (5.7.2016).

<sup>20</sup> <http://ec.europa.eu/info/law/better-regulation/initiatives/Ares-2017-3971182>.

<sup>21</sup> La Decisión marco 2006/960/JAI del Consejo (la llamada «iniciativa sueca») contempla los plazos siguientes para la respuesta de las autoridades policiales a los requerimientos de otros países: ocho horas en casos urgentes en los que la información o la inteligencia solicitada se conserve en una base de datos

El acceso a los datos sobre transacciones financieras en poder de otros Estados miembros puede asimismo facilitarse a través de las unidades de inteligencia financiera. Cuando esa información deba utilizarse como prueba en un proceso penal, posiblemente deba requerirse a través de un procedimiento de asistencia judicial. La orden europea de investigación<sup>22</sup> ofrece nuevas posibilidades de obtener datos sobre transacciones financieras de forma considerablemente más rápida que a través de la asistencia judicial. Hasta la fecha, transcurridos algunos meses desde el final del plazo de transposición, tan solo 16 Estados miembros han incorporado a su ordenamiento interno la orden europea de investigación. Se insta a los demás a hacerlo de inmediato. Por último, las propuestas legislativas sobre pruebas electrónicas previstas para el principio de 2018 facilitarán también el acceso transfronterizo a esos datos.

Las consultas con los interesados señalan también la existencia de **obstáculos que entorpecen la detección de los datos sobre transacciones financieras conservados en otros Estados miembros**. Como paso hacia la solución de este problema y como parte de su evaluación en curso, la Comisión estudiará la necesidad, la viabilidad técnica y la proporcionalidad de la interconexión de los registros centrales de cuentas bancarias, tomando en consideración todos los instrumentos existentes y previstos para facilitar el acceso a los datos sobre transacciones financieras en poder de otros Estados miembros.

Con ese fin, la Comisión **proseguirá sus consultas con todas las partes interesadas** acerca de la necesidad, la viabilidad técnica y la proporcionalidad de las posibles nuevas medidas de la Unión para facilitar y acelerar el acceso a los datos sobre transacciones financieras, incluidos los procedimientos destinados a garantizar su confidencialidad. En noviembre de 2017, una vez reunidas todas las evaluaciones en curso sobre el uso de la información financiera en las investigaciones antiterroristas, la Comisión organizará una reunión de alto nivel con los interesados. Entre los grandes temas de debate se incluirán los siguientes:

- los principales obstáculos a un acceso efectivo y en tiempo oportuno a los datos sobre transacciones financieras en poder de otros Estados miembros con miras a investigaciones antiterroristas;
- la necesidad, viabilidad técnica y proporcionalidad de las posibles medidas adicionales para facilitar de forma rápida, eficaz y segura el acceso transfronterizo a datos sobre transacciones financieras con miras a investigaciones antiterroristas.

La Comisión informará sobre las conclusiones de este debate.

## 2. *Explosivos: aumento de las restricciones de acceso a los precursores de explosivos*

El **Reglamento sobre los precursores de explosivos**<sup>23</sup> restringe el acceso del público y la utilización por su parte de siete sustancias químicas (los llamados precursores de explosivos restringidos que se enumeran en el anexo I del Reglamento). En febrero de 2017, la Comisión adoptó un informe sobre la aplicación del Reglamento por los Estados miembros<sup>24</sup>. En él se concluía que ha contribuido a reducir el acceso a los precursores de explosivos peligrosos que

---

directamente accesible por esas autoridades; plazos más largos cuando dicha información o inteligencia no se conserve en una base de datos directamente accesible.

<sup>22</sup> Directiva 2014/41/CE (3.4.2014).

<sup>23</sup> Reglamento 98/2013/CE (15.1.2013).

<sup>24</sup> COM(2017) 103 final (28.2.2017).



pueden utilizarse con fines adversos, a saber, la fabricación de explosivos caseros. Los Estados miembros también presentaron ejemplos de detección temprana de tramas terroristas merced a la aplicación del Reglamento<sup>25</sup>. Para asegurar su plena aplicación, la Comisión incoó en mayo y septiembre de 2016 procedimientos de infracción contra determinados Estados miembros que no habían cumplido esa obligación. En octubre de 2017 solo quedaban dos procedimientos de infracción activos: contra España y contra Rumanía.

A pesar de estos esfuerzos conjuntos, los recientes atentados e incidentes terroristas indican que la **amenaza planteada por los explosivos de fabricación casera** sigue siendo elevada. Persiste el acceso a estas sustancias y su uso para la fabricación de explosivos caseros. El explosivo utilizado en la mayoría de los atentados fue el triperóxido de triacetona (TATP), sustancia de fabricación casera por la que, al parecer, tienen predilección los terroristas<sup>26</sup>.

Habida cuenta de la amenaza que plantean actualmente los precursores de explosivos, es necesario actuar de inmediato para asegurar que todos los Estados apliquen el Reglamento vigente con la máxima diligencia. Por ello, la Comisión ha publicado, junto con el presente informe, una **Recomendación**<sup>27</sup> en la que ofrece orientaciones sobre las medidas que deben adoptarse inmediatamente para impedir el uso indebido de los precursores de explosivos. La Comisión anima a los Estados miembros a que apliquen todos los puntos de dicha Recomendación para restringir en la mayor medida posible el acceso a los precursores de explosivos y el uso de los mismos por terroristas y asegurar la mejora de los controles de los usos legítimos y la adopción de medidas en caso de transacciones sospechosas. La Comisión se mantiene dispuesta a ayudar a los Estados miembros a llevar a cabo ese cometido.

Además, la Comisión se propone intensificar su **revisión del Reglamento sobre precursores de explosivos** mediante un análisis que irá seguido de una evaluación de impacto durante el primer semestre de 2018. El análisis examinará la pertinencia, eficacia, eficiencia, coherencia y valor añadido del Reglamento, y determinará los problemas y obstáculos que podrían reclamar la adopción de nuevas medidas. La evaluación de impacto examinará las distintas opciones de actuación para resolver los problemas y obstáculos detectados.

### 3. *Cifrado: ayuda a las autoridades policiales y judiciales en sus investigaciones penales*

El uso del cifrado es esencial para asegurar la ciberseguridad y la protección de los datos personales. La legislación de la UE recoge específicamente la función del cifrado para garantizar un nivel apropiado de seguridad en el tratamiento de datos personales<sup>28</sup>. Al mismo tiempo, las autoridades policiales y judiciales cada vez tropiezan, en sus investigaciones penales, con más escollos derivados del uso del cifrado por los delincuentes. Ello afecta a su capacidad para obtener la información que necesitan como prueba en sus investigaciones penales y para enjuiciar y condenar a los delincuentes. Está previsto que el uso del cifrado por los delincuentes y su impacto en las investigaciones penales sigan aumentando en los próximos años.

---

<sup>25</sup> El 23 de junio de 2017, el ministro de interior belga anunció que, en el espacio de un año, se habían recibido 30 notificaciones de ventas sospechosas. Entre febrero y junio de 2017, Francia recibió 11 notificaciones, casi todas ellas relativas al peróxido de hidrógeno.

<sup>26</sup> Informe sobre la situación y las tendencias del terrorismo en la UE (TE-SAT), 2017 <https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report-te-sat-2017>.

<sup>27</sup> COM(2017) 6950 final (18.10.2017).

<sup>28</sup> Artículo 32 del Reglamento 2016/679/CE (27.4.2017).

Atendiendo la petición del Consejo de Justicia y Asuntos de Interior de diciembre de 2016, la Comisión **discutió con las partes interesadas el papel del cifrado en las investigaciones penales**, abordando sus aspectos tanto técnicos como jurídicos. Se trataba de expertos de Europol, Eurojust, la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA), la Agencia de los Derechos Fundamentales de la Unión Europea (FRA), los cuerpos de seguridad de los Estados miembros, la industria y las organizaciones de la sociedad civil. Los progresos se notificaron con regularidad en el grupo de trabajo del Consejo y el 18 de septiembre de 2017 se llevó a cabo un taller con los Estados miembros. A lo largo del proceso, se celebraron diversas mesas redondas con la industria y las organizaciones de la sociedad civil.

Tras este debate con los Estados miembros y las partes interesadas, y teniendo en cuenta su aportación, la Comisión concluye que es preciso aplicar el siguiente conjunto de **medidas de asistencia a las autoridades policiales y judiciales** que, en el transcurso de sus investigaciones penales, encuentren información cifrada por los delincuentes. Se trata de a) medidas legales para facilitar el acceso a pruebas cifradas y de b) medidas técnicas para reforzar las capacidades de descifrado. La Comisión seguirá vigilando la evolución de esta situación.

*a) marco jurídico del acceso transfronterizo a las pruebas electrónicas*

Las autoridades policiales y judiciales tropiezan a menudo con la dificultad de acceder a pruebas situadas en otro país. Los actuales cambios en la legislación europea permiten ampliar las atribuciones de las autoridades policiales y judiciales para obtener acceso a información necesaria –si bien posiblemente encriptada– situada en otro Estado miembro. La investigación y el enjuiciamiento efectivo de los delitos necesitan un marco apropiado. Con ese fin, la Comisión presentará al principio de 2018 propuestas destinadas a facilitar el **acceso transfronterizo a las pruebas electrónicas**. En paralelo, la Comisión está aplicando un conjunto de medidas prácticas<sup>29</sup> para mejorar el acceso transfronterizo a las pruebas electrónicas en el marco de investigaciones criminales, entre las que se incluye la financiación de formación sobre cooperación transfronteriza, el desarrollo de una plataforma electrónica de intercambio de información dentro de la UE y la normalización de los formularios para la cooperación judicial entre Estados miembros.

*b) medidas técnicas*

Dependiendo de los métodos de cifrado empleados por los delincuentes, las autoridades policiales y judiciales consiguen recuperar parte de la información. Algunos Estados miembros han creado servicios nacionales con especialistas que se enfrentan al reto de la información cifrada en el contexto de las investigaciones penales. No obstante, la mayor parte de los Estados miembros no tienen acceso al nivel de conocimientos especializados ni a los recursos técnicos adecuados, lo que compromete seriamente la capacidad de las autoridades policiales y judiciales para acceder a la información encriptada en las investigaciones penales. La Comisión propone, por ese motivo, un **conjunto de medidas de asistencia a las autoridades de los Estados miembros**, que no implican la prohibición, limitación ni debilitamiento del cifrado.

---

<sup>29</sup> Véase el Octavo informe de situación relativo a una Unión de la Seguridad genuina y efectiva (COM(2017) 354 final de 29.6.2017).

En primer lugar, la Comisión ayudará a **Europol** a seguir desarrollando su capacidad de descifrado, con cuyo fin ha propuesto para este organismo, en el ejercicio de preparación del presupuesto de la UE para 2018, un total de 86 puestos adicionales relacionados con la seguridad (19 más que en el presupuesto de 2017), con el objetivo concreto de reforzar el Centro Europeo de Ciberdelincuencia (EC3) de Europol. Se estudiará la necesidad de recursos adicionales y, en el próximo informe de evolución hacia una Unión de la Seguridad, la Comisión notificará los fondos destinados a esas partidas. El desarrollo tecnológico futuro deberá tenerse en cuenta en las actividades de investigación y desarrollo enmarcadas en el programa Horizonte 2020 y otros programas financiados por la UE. No se tomarán en consideración aquellas medidas que puedan debilitar el cifrado o repercutir en un número de personas más amplio o indiscriminado.

En segundo lugar, el apoyo a las autoridades policiales y judiciales a escala nacional requiere el establecimiento de una **red de puntos de expertos** que, sin suplantar las iniciativas nacionales, facilite una mejor puesta en común de las capacidades y los conocimientos especializados nacionales. Se anima a los Estados miembros a utilizar la financiación correspondiente a los programas del Fondo de Seguridad Interior - Policía para crear, ampliar o desarrollar los puntos de expertos nacionales. A escala europea, la Comisión ayudará a Europol a desempeñar las funciones de plataforma de red para facilitar la colaboración entre estos puntos de expertos nacionales.

En tercer lugar, será preciso poner a disposición de las autoridades de los Estados miembros un **instrumental de técnicas de investigación alternativas** que facilite el desarrollo y la aplicación de medidas para la obtención de la información necesaria cifrada por los delincuentes. La red de puntos de expertos habrá de contribuir a la creación de este instrumental, siendo el Centro Europeo de Ciberdelincuencia (EC3) de Europol el organismo más apropiado para crear y mantener un repositorio de esas técnicas y herramientas. No se tomarán en consideración aquellas medidas que puedan debilitar el cifrado o repercutir en un número de personas más amplio o indiscriminado.

En cuarto lugar, habrá que prestar atención al **importante papel de los proveedores de servicios y otros interlocutores industriales** para aportar soluciones en cuanto al cifrado de alto nivel. Habida cuenta del compromiso de la Comisión con el cifrado de alto nivel, la existencia de una colaboración más rica y estructurada entre autoridades, proveedores de servicios y otros interlocutores industriales favorecería una mejor comprensión de los desafíos actuales y cambiantes. La Comisión promoverá diálogos estructurados con los proveedores de servicios y otras empresas en el marco del Foro de Internet de la UE y la red de puntos de expertos, con la participación, cuando proceda, de la sociedad civil.

En quinto lugar, será preciso asegurar, mediante **programas de formación** destinados a autoridades policiales y judiciales, que los agentes y funcionarios responsables están mejor preparados para obtener la información necesaria cifrada por los delincuentes. Para apoyar el desarrollo de programas de formación, la Comisión se propone aportar fondos por un importe de 500 000 EUR con cargo al programa de trabajo anual de 2018 del Fondo de Seguridad Interior - Policía. Se tendrán en cuenta, siempre que sea pertinente, los conocimientos especializados del Grupo Europeo de Formación y Educación en Ciberdelincuencia (ECTEG). La Comisión respaldará además la impartición de formación por la Agencia de la Unión Europea para la Formación Policial (CEPOL); se recomienda a los Estados miembros que

destinen a formación los fondos disponibles en sus programas nacionales del Fondo de Seguridad Interior - Policía.

En sexto lugar, se ha constatado la necesidad de una **evaluación continua de los aspectos técnicos y jurídicos** del papel del cifrado en las investigaciones penales, habida cuenta del constante desarrollo de técnicas de cifrado, del incremento de su uso por los delincuentes y de los efectos de estos fenómenos en las investigaciones penales. La Comisión perseverará en esta importante labor. Además, propiciará el desarrollo de una función de observatorio en colaboración con el Centro Europeo de Ciberdelincuencia (EC3) de Europol, la Red Judicial Europea sobre Ciberdelincuencia (EJCN) y Eurojust.

#### **IV. Lucha contra la radicalización**

##### *1. Grupo de Expertos de Alto Nivel sobre radicalización*

Los recientes atentados, especialmente los perpetrados por agentes solitarios, y la rapidez de la radicalización de sus autores nos han recordado brutalmente la importancia de prevenir y contrarrestar la radicalización. La Comisión ha establecido un **Grupo de Expertos de Alto Nivel sobre radicalización** que intensificará los esfuerzos para prevenir y contrarrestar la radicalización y que, partiendo de los logros alcanzados hasta la fecha, mejore la coordinación y la cooperación entre todos los interlocutores<sup>30</sup>. Se le ha encomendado la formulación de recomendaciones de actuación en este campo, debiendo asimismo presentar un primer informe intermedio este año. La Comisión expondrá ante el Consejo de Justicia y Asuntos de Interior de diciembre de 2017 los progresos alcanzados. El Grupo abordará asimismo el marco de condiciones necesario para reforzar la capacidad y los conocimientos especializados en materia de lucha contra la radicalización, incluida la posible creación de nuevas estructuras de cooperación al nivel de la UE. A este propósito, algunos Estados miembros han reclamado la creación de un centro de prevención de la radicalización de la UE, cuya necesidad y valor añadido examinará también el Grupo.

Una de las cuestiones prioritarias que ha de tratar el Grupo es la **radicalización en las cárceles**. La actividad se centra actualmente en la aplicación, por parte de los Estados miembros, de las conclusiones del Consejo de JAI de 20 de noviembre de 2015 sobre la mejora de la respuesta de la justicia penal a la radicalización<sup>31</sup>. El 27 de febrero de 2018, la Comisión organizará una conferencia de las partes interesadas sobre la respuesta de la justicia penal a la radicalización, en la que se pondrán en común los resultados de los proyectos en curso.

La Comisión tendrá en cuenta las conclusiones y recomendaciones del Grupo en el programa de trabajo de las iniciativas existentes (especialmente las del Centro de Excelencia de la Red para la Sensibilización frente a la Radicalización), así como en el uso y los fines de sus instrumentos de financiación (incluidos el Fondo de Seguridad Interior y otros fondos relacionados con este como Erasmus+, el programa de Justicia o el Fondo Social Europeo).

##### *2. Lucha contra la radicalización en línea*

---

<sup>30</sup> Véase el Octavo informe de situación relativo a una Unión de la Seguridad genuina y efectiva (COM(2017) 354 final de 29.7.2017).

<sup>31</sup> Conclusiones del Consejo de la Unión Europea y de los Estados miembros reunidos en el seno del Consejo, sobre la mejora de la respuesta de la justicia penal a la radicalización que conduce al terrorismo y al extremismo violento (14382/15).

Los terroristas siguen utilizando Internet con fines de radicalización, captación, preparación de sus atentados, incitación a los mismos y ensalzamiento de sus atrocidades. El Consejo Europeo<sup>32</sup>, el G7<sup>33</sup> y el G20<sup>34</sup> han reclamado recientemente nuevas actuaciones para abordar este desafío global y han recordado la responsabilidad del sector industrial a este respecto.

En julio de 2017, el Foro de Internet de la UE expuso su **Plan de acción para luchar contra el contenido terrorista en línea**, en el que instaba a las empresas de Internet a que adoptaran medidas decisivas, dedicaran los recursos suficientes y desarrollaran las herramientas tecnológicas necesarias para asegurar la rápida detección y retirada de material pernicioso. El Plan de acción exige avances inmediatos en una serie de aspectos<sup>35</sup> y fija un mecanismo de notificación periódica que permite describir las medidas y evaluar los resultados.

El 29 de septiembre de 2017, la Comisión organizó una reunión de altos funcionarios del Foro de Internet de la UE para hacer balance de la **aplicación del Plan de acción para luchar contra el contenido terrorista en línea**. Por lo que se refiere a la detección automática, cada vez son más las empresas que avanzan en esa dirección, que les permite desplegar sus técnicas de detección de contenido terrorista en el punto en que este ha sido cargado. Algunas de ellas han indicado que un 75 % del contenido ya se detecta automáticamente (y se transmite a revisores humanos, quienes adoptan la decisión final sobre su retirada), mientras que otras señalan que un 95 % del contenido se detecta mediante sistemas de detección patentados. Si bien los progresos alcanzados son palpables, la Comisión ha instado a todas las empresas a que agilicen el despliegue de estas herramientas para acelerar la detección del contenido terrorista, reducir el tiempo que este permanece en línea y proceder a una retirada más rápida y eficaz de este tipo de propaganda. La Comisión también les ha solicitado encarecidamente que amplíen su mecanismo de «base de datos de hash» para asegurar que el contenido terrorista retirado no se vuelva a cargar en otras plataformas, atajando de ese modo la difusión de contenido terrorista en múltiples plataformas. Ese mecanismo debe ampliarse en una doble dirección: en cuanto al contenido que incluye (que debe ir más allá de los vídeos y las imágenes que abarca actualmente) y en cuanto a las empresas participantes.

La Comisión sigue ofreciendo su apoyo a las organizaciones de la sociedad civil para que divulguen **mensajes que configuren un relato alternativo** en línea. El 6 de octubre de 2017, la Comisión publicó una convocatoria de propuestas con el propósito de aportar fondos por un valor de 6 millones EUR a los consorcios de agentes de la sociedad civil que desarrollen y ejecuten este tipo de campañas.

El 6 de diciembre de 2017, la Comisión Europea convocará al **Foro de Internet de la UE a nivel ministerial**, en el que participarán altos representantes de las empresas de Internet y en el que se preparará la vía de actuación futura.

Las medidas adoptadas contra el contenido terrorista en línea en el marco del Foro de Internet de la UE deben interpretarse en el contexto más amplio de la lucha contra el contenido ilegal en Internet. Estas medidas fueron reforzadas por una Comunicación adoptada por la Comisión el 28 de septiembre de 2017 en la que se establecieron las **directrices y los principios aplicables a las plataformas en línea** a fin de intensificar la lucha contra el contenido ilegal

<sup>32</sup> [http://www.consilium.europa.eu/en/meetings/european-council/2017/06/22-23-euco-conclusions\\_pdf/](http://www.consilium.europa.eu/en/meetings/european-council/2017/06/22-23-euco-conclusions_pdf/).

<sup>33</sup> <http://www.consilium.europa.eu/en/press/press-releases/2017/05/26-statement-fight-against-terrorism/>.

<sup>34</sup> <http://www.consilium.europa.eu/en/press/press-releases/2017/07/07-g20-counter-terrorism/>.

<sup>35</sup> COM(2017) 407 final (26.7.2017).

en línea<sup>36</sup> en cooperación con las autoridades nacionales, los Estados miembros y otras partes interesadas. La Comunicación pretende facilitar e intensificar la aplicación de las buenas prácticas de prevención, detección, eliminación y supresión del acceso al contenido ilegal con el fin de asegurar la retirada efectiva de este tipo de contenido, aumentar la transparencia y proteger los derechos fundamentales. Se propone también ofrecer a las plataformas aclaraciones en cuanto a su responsabilidad a la hora de tomar medidas proactivas para detectar contenido ilegal, retirarlo o suprimir el acceso al mismo. La Comisión espera que, en los próximos meses, las plataformas en línea actúen con rapidez, también en el contexto de los marcos de diálogo pertinentes como el Foro de Internet de la UE sobre el terrorismo y la incitación al odio.

En paralelo, la Comisión seguirá supervisando los progresos alcanzados y determinando si se necesitan medidas adicionales para asegurar la detección y retirada rápidas y proactivas del contenido ilegal en línea, entre las que pueden contarse medidas legislativas que complementen el marco normativo vigente. Este trabajo concluirá en mayo de 2018.

En la vertiente legislativa, la propuesta de la Comisión<sup>37</sup> para la **revisión de la Directiva de servicios de comunicación audiovisual**, presentada en mayo de 2016, intensifica la lucha contra la incitación al odio. Pretende alinear dicha Directiva con la Decisión marco relativa a la lucha contra determinadas formas y manifestaciones de racismo y xenofobia<sup>38</sup> y con la Carta de los Derechos Fundamentales. Contempla asimismo la obligación, para los Estados miembros, de asegurar que las plataformas de distribución de vídeos implanten las medidas adecuadas para proteger a todos los ciudadanos de la incitación a la violencia o al odio, que pueden consistir, por ejemplo, en mecanismos de señalización y denuncia.

## V. DIMENSIÓN EXTERIOR DE LA LUCHA CONTRA EL TERRORISMO

### 1. *Acción exterior de la UE contra el terrorismo*

La acción exterior de la UE contra el terrorismo contribuye al objetivo prioritario de reforzar la seguridad interior de la UE. Por consiguiente, es preciso seguir fortaleciendo el continuo estratégico y político entre la seguridad interior y la seguridad exterior para potenciar la eficacia de las medidas de lucha contra el terrorismo en todos los frentes.

La Comisión presta su apoyo a un amplio espectro de medidas exteriores de refuerzo de la seguridad y ha destinado fondos por un valor superior a 2 300 millones EUR a más de 600 proyectos en curso a 1 de enero de 2017. Algunas de esas actividades se centran en la seguridad (son, por ejemplo, medidas concretas contra la financiación del terrorismo o la radicalización, o medidas referentes a las fronteras o las prisiones), o inciden en ella (por ejemplo, programas que abordan las causas originales de la inseguridad o de los agravios contribuyendo a mejorar la educación, el acceso a los recursos naturales y la energía, la gobernanza y el sector de la seguridad y el apoyo a la sociedad civil).

El Consejo de Asuntos Exteriores de 19 de junio de 2017 renovó la orientación estratégica en estos ámbitos mediante la adopción de las **Conclusiones del Consejo sobre la acción**

---

<sup>36</sup> Comunicación sobre la lucha contra los contenidos ilegales en línea y la mayor responsabilidad de las plataformas en línea (COM(2017) 555 final de 28.9.2017).

<sup>37</sup> COM(2016) 287 final (25.5.2016).

<sup>38</sup> Decisión marco 2008/913/JAI del Consejo (28.11.2008).

**exterior de la UE en materia de lucha contra el terrorismo**<sup>39</sup>, de carácter integral. La alta representante y la Comisión Europea trabajarán conjuntamente en la medida necesaria para la satisfactoria aplicación de estas Conclusiones. A fin de asegurar la puntualidad y el rigor en la aplicación de las Conclusiones y en la presentación del correspondiente informe al Consejo antes del final de junio de 2018, se ha establecido un proceso de coordinación conjunto entre el Servicio Europeo de Acción Exterior y la Comisión Europea. Se otorgará prioridad a las iniciativas siguientes:

- **Reforzar la red de expertos en la lucha antiterrorista en las Delegaciones de la UE:** estos expertos deberán estar cada vez más implicados en la programación de la ayuda de la UE y en la coordinación local de los programas individuales de cooperación antiterrorismo de los Estados miembros con nuestros socios. Para favorecer el ejercicio de estas responsabilidades acrecentadas, se intensificará la formación previa y simultánea al despliegue de estos expertos. Su cometido será más concreto y se definirá en cartas de misión específicas, y su vinculación con las agencias de Justicia y Asuntos de Interior de la UE se hará más estable. Para abarcar todas las zonas de máxima prioridad, la red de expertos en la lucha antiterrorista<sup>40</sup> se expandirá al Cuerno de África, Asia Central y Asia Sudoriental.
- **Aumentar la cooperación entre las misiones y operaciones de la Política Común de Seguridad y Defensa y las agencias de Justicia y Asuntos de Interior de la UE** con fines de recogida, análisis e intercambio de información, y explorar las posibilidades de mejora de las conexiones entre los agentes militares y las autoridades policiales para la lucha antiterrorista. Para potenciar el intercambio de datos e información entre la Política Común de Seguridad y Defensa y las políticas de justicia y asuntos de interior, será importante propiciar una revisión de los elementos que componen los marcos normativos vigentes y orientar la inserción de células de información sobre delincuencia en determinadas misiones y operaciones de la Política Común de Seguridad y Defensa. También lo será facilitar y mejorar los vínculos con las actividades de las agencias de Justicia y Asuntos de Interior de la UE en los terceros países prioritarios, aumentando, siempre que sea posible, el intercambio de información entre los agentes de la UE y los agentes externos.
- **Robustecer la cooperación internacional para la lucha contra el terrorismo y la prevención y el rechazo del extremismo violento** con nuestros países socios en los Balcanes Occidentales, Oriente Medio, África del Norte, Turquía y los países del Golfo, el Sahel y el Cuerno de África; con nuestros principales socios estratégicos, entre los que se cuentan los Estados Unidos, Canadá y Australia, y con interlocutores regionales y multilaterales fundamentales como las Naciones Unidas, la OTAN, el Foro Mundial contra el Terrorismo, el Grupo de Acción Financiera Internacional, la Unión Africana, la Asociación de Naciones del Asia Sudoriental, el Consejo de Cooperación del Golfo y la Liga de Estados Árabes.

## 2. *Convenio del Consejo de Europa para la prevención del terrorismo*

---

<sup>39</sup> [http://www.consilium.europa.eu/en/press/press-releases/2017/06/pdf/Read-the-full-text-of-the-Council-conclusions\\_pdf\(4\)/](http://www.consilium.europa.eu/en/press/press-releases/2017/06/pdf/Read-the-full-text-of-the-Council-conclusions_pdf(4)/).

<sup>40</sup> Actualmente, la UE ha enviado expertos de este tipo a sus delegaciones en: Arabia Saudí, Argelia, Bosnia y Herzegovina (con un mandato regional para los Balcanes Occidentales), Chad (Sahel), Irak, Jordania, Líbano, Libia (destacamento en Túnez), Marruecos, Nigeria, Pakistán, Túnez y Turquía.

Para reforzar la cooperación internacional en la lucha contra el terrorismo, la Comisión presenta, en paralelo a este informe, **propuestas<sup>41</sup> de Decisiones del Consejo sobre la celebración del Convenio del Consejo de Europa para la prevención del terrorismo y su Protocolo adicional**. El Convenio<sup>42</sup>, adoptado por el Consejo de Europa el 16 de mayo de 2005, abarca cuestiones como la tipificación penal de las actividades terroristas y afines, la cooperación internacional relacionada con esos delitos, y la protección, indemnización y ayuda a las víctimas del terrorismo. El Convenio entró en vigor el 1 de junio de 2007. Todos los Estados miembros de la UE lo han firmado y 23 de ellos lo han ratificado. El objetivo del Protocolo adicional<sup>43</sup>, adoptado por el Consejo de Europa el 18 de mayo de 2015, es completar el Convenio con una serie de disposiciones por las que se aplican los aspectos de Derecho penal de la Resolución del Consejo de las Naciones Unidas 2178(2014)<sup>44</sup> titulada «Amenazas a la paz y la seguridad internacionales causadas por actos terroristas». El Protocolo adicional responde a esta Resolución configurando una interpretación y una respuesta comunes en relación con los delitos de los combatientes terroristas extranjeros. El Protocolo adicional entró en vigor el 1 de julio de 2017.

La UE firmó el Convenio y su Protocolo adicional el 22 de octubre de 2015. Tras la adopción de una panoplia completa de instrumentos jurídicos para plantar cara al terrorismo, entre los que figura la Directiva sobre la lucha contra el terrorismo<sup>45</sup>, la UE está ahora preparada para cumplir su compromiso, pasando a ser parte del Convenio y su Protocolo adicional.

### 3. *Hacia la revisión del Acuerdo sobre el registro de nombres de los pasajeros con Canadá*

En su dictamen de 26 de julio de 2017<sup>46</sup>, el Tribunal de Justicia de la UE declaró que el Acuerdo entre Canadá y la UE sobre la transferencia y el uso del registro de nombres de los pasajeros (PNR), firmado el 25 de junio de 2014, no podía celebrarse en su forma actual dado que algunas de sus disposiciones son incompatibles con los derechos fundamentales de la UE, en particular el derecho a la protección de los datos y el respeto a la vida privada. La Comisión mantiene ahora contactos con Canadá —que se prolongarán en paralelo a la próxima reunión de ministros de Interior del G7 que se celebrará en Ischia los días 19 y 20 de octubre de 2017— con el fin de preparar las inminentes negociaciones de revisión del texto del Acuerdo. Para ello, la Comisión ha presentado, junto a este informe, una **Recomendación al Consejo<sup>47</sup> por la que se autoriza la apertura de negociaciones para la revisión del Acuerdo** con arreglo a los requisitos fijados por el Tribunal en su dictamen. Se ruega al Consejo que autorice sin demora la apertura de dichas negociaciones. Dado que el uso de los datos PNR es un arma decisiva en la lucha contra el terrorismo y las formas graves de delincuencia transnacional, la Comisión adoptará las medidas necesarias para garantizar la continuidad de las transferencias de datos PNR a Canadá en estricto respeto de los derechos fundamentales, de conformidad con el dictamen del Tribunal.

---

<sup>41</sup> COM(2017) 606 final (18.10.2017) y COM(2017) 607 final (18.10.2017).

<sup>42</sup> <https://rm.coe.int/168008371c>.

<sup>43</sup> <https://rm.coe.int/168047c5ea>.

<sup>44</sup> [http://www.un.org/en/sc/ctc/docs/2015/SCR%202178\\_2014\\_EN.pdf](http://www.un.org/en/sc/ctc/docs/2015/SCR%202178_2014_EN.pdf).

<sup>45</sup> Directiva 2017/541/CE (15.3.2017).

<sup>46</sup> Dictamen 1/15 del Tribunal de Justicia (26.7.2017)

<sup>47</sup> COM(2017) 605 final (18.10.2017).



En este contexto, la Comisión desea hacer constar su permanente apoyo a los Estados miembros en cuanto a la aplicación de la Directiva relativa al registro de nombres de los pasajeros<sup>48</sup>; las obligaciones que de ella dimanaban para los Estados miembros no se ven afectadas por el dictamen del Tribunal.

#### 4. *Refuerzo de la cooperación de Interpol con terceros países*

La cooperación con terceros países es esencial para la lucha contra el terrorismo y la delincuencia organizada, según subrayan las Conclusiones del Consejo de Asuntos Exteriores de Junio de 2017 sobre la acción exterior de la UE en materia de lucha contra el terrorismo<sup>49</sup>, así como para las estrategias regionales pertinentes de la UE<sup>50</sup>. Antes de la entrada en vigor del nuevo Reglamento de Europol<sup>51</sup>, el 1 de mayo de 2017, este organismo había celebrado, con arreglo a su base jurídica anterior<sup>52</sup>, una serie de acuerdos con terceros países con el fin de asegurar la existencia de un marco de cooperación para el intercambio de información estratégica y técnica. Algunos de esos acuerdos incluyen también la posibilidad de intercambiar datos personales<sup>53</sup>. Tales acuerdos permanecen en vigor.

Desde el 1 de mayo de 2017, el nuevo **Reglamento de Europol** contiene las disposiciones por las que se rigen las relaciones exteriores de este organismo con terceros países y, en particular, las condiciones para el intercambio de datos personales con organismos de la Unión, terceros países y organizaciones internacionales. De conformidad con el Tratado y con el citado Reglamento, la Comisión es responsable, en nombre de la Unión, de negociar los acuerdos internacionales con terceros países para el intercambio de datos con Europol<sup>54</sup>. En la medida que sea necesaria para el desempeño de su cometido, Europol puede establecer y mantener con socios exteriores relaciones de cooperación basadas en disposiciones administrativas que no permitan el intercambio de datos personales.

Habida cuenta de las necesidades operativas de la Unión en cuanto a la cooperación en materia de seguridad con terceros países, y de acuerdo con el Reglamento de Europol, la **Comisión presentará al Consejo, antes de que termine el año, una serie de recomendaciones para** que autorice la apertura de negociaciones dirigidas a la celebración de acuerdos entre la UE y Argelia, Egipto, Israel, Jordania, Líbano, Marruecos, Túnez y Turquía que sienten las bases jurídicas para la transferencia de datos entre Europol y esos terceros países<sup>55</sup>. Esos acuerdos reforzarán las capacidades de interacción de Europol con

---

<sup>48</sup> Directiva 2016/681/CE (27.4.2016).

<sup>49</sup> [http://www.consilium.europa.eu/en/press/press-releases/2017/06/pdf/Read-the-full-text-of-the-Council-conclusions\\_pdf\(4\)/](http://www.consilium.europa.eu/en/press/press-releases/2017/06/pdf/Read-the-full-text-of-the-Council-conclusions_pdf(4)/).

<sup>50</sup> Incluida la Política Europea de Vecindad revisada, (JOIN(2015) 50 final de 18.11.2015).

<sup>51</sup> Reglamento 2016/794/CE (11.5.2016).

<sup>52</sup> Decisión 2009/371/JAI del Consejo (6.4.2009).

<sup>53</sup> Europol ha celebrado acuerdos que contemplan el intercambio de datos personales con los terceros países siguientes: Albania, Antigua República Yugoslava de Macedonia, Australia, Bosnia y Herzegovina, Canadá, Colombia, Georgia, Islandia, Liechtenstein, Moldavia, Mónaco, Montenegro, Noruega, Serbia, Suiza, Ucrania y los Estados Unidos. El Consejo de Administración de Europol había autorizado la apertura de negociaciones para la celebración de un acuerdo entre Europol e Israel, negociaciones que no habían concluido cuando entró en vigor el nuevo Reglamento de Europol.

<sup>54</sup> El Reglamento de Europol contempla asimismo la transferencia de datos personales entre Europol y un tercer país, previa Decisión de la Comisión que determine que dicho país ofrece un nivel de protección de datos adecuado («decisión de adecuación»).

<sup>55</sup> Además de las relaciones con estos países, la Comisión desea recordar el marco estratégico que constituyen las «decisiones de adecuación» y demás instrumentos de transferencia de datos y protección internacional,

estos terceros países con el fin de prevenir y combatir los delitos que están en el punto de mira de Europol.

## **VI. CONCLUSIÓN**

Este informe presenta un paquete de medidas de lucha contra el terrorismo con las que se seguirá apoyando a los Estados miembros en su esfuerzo por hacer frente a las actuales amenazas a la seguridad. La Comisión recomienda a los Estados miembros y al Consejo que las apliquen con carácter prioritario. Mantendrá informados al Parlamento Europeo y al Consejo de los progresos realizados.

El próximo informe de evolución hacia una Unión de la Seguridad genuina y efectiva se presentará en diciembre de 2017 y se centrará en la interoperabilidad de los sistemas de información con vistas a la gestión de la seguridad, las fronteras y la migración. La Comisión recuerda en este contexto la importancia de avanzar en las prioridades legislativas relativas a estos sistemas de información.

---

conforme se precisa en la Comunicación de la Comisión sobre el intercambio y la protección de los datos personales en un mundo globalizado (COM(2017) 7 final de 10.1.2017), en la que la Comisión recomienda encarecidamente la adhesión de terceros países al Convenio del Consejo de Europa 108 y su Protocolo adicional.