COMISIÓN
EUROPEA

Bruselas, 25.1.2017
COM(2017) 41 final

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

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

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

I. INTRODUCCIÓN

El presente es el cuarto informe mensual sobre los progresos realizados hacia una Unión de la Seguridad genuina y efectiva y abarca la evolución de los acontecimientos en dos pilares principales: *la lucha contra el terrorismo y la delincuencia organizada y contra los medios que los sustentan y el fortalecimiento de nuestras defensas y de nuestra resiliencia frente a estas amenazas*. El presente informe se centra en cuatro ámbitos fundamentales, a saber, los sistemas de información y la interoperabilidad, la protección de objetivos no militares o indefensos, la amenaza cibernética y la protección de los datos en el marco de las investigaciones penales.

El ataque del mercado de Navidad de Berlín del pasado diciembre puso de manifiesto de nuevo las graves deficiencias de nuestros sistemas de información que es necesario subsanar urgentemente, en especial a nivel de la UE, para ayudar a la policía aduanera y fuerzas y cuerpos de seguridad nacionales sobre el terreno a realizar su exigente trabajo con mayor eficacia. El hecho de que los distintos sistemas de información no estén interconectados (lo que permite que los autores de los ataques utilicen identidades múltiples y se desplacen sin ser detectados, incluso al cruzar fronteras) y de que esa información no sea cargada sistemáticamente por los Estados miembros en las bases de datos de la UE son deficiencias prácticas de ejecución que deben subsanarse urgentemente. Además, es necesario seguir trabajando[1] en lo relativo a las medidas policiales en las fronteras y el retorno a su país de las personas cuyas peticiones de asilo se hayan denegado.

En cuanto a la protección de objetivos no militares, la Comisión acelerará el trabajo que está realizando para reunir a expertos de los Estados miembros con el fin de intercambiar mejores prácticas y acordar directrices comunes.

La amenaza cibernética que afronta la UE es objeto de una amplia cobertura en los medios de comunicación, y el presente informe pasa revista a las diversas líneas de trabajo ya en curso en este ámbito. Se trata, por un lado, de prevenir, — trabajando con la industria para promover la seguridad mediante el diseño y la puesta en práctica de la Directiva sobre Seguridad de las Redes de Información — y, por otro, de impulsar la cooperación entre los Estados miembros y con las organizaciones y los socios internacionales sobre cómo hacer frente a los ataques informáticos a medida que se produzcan. En los próximos meses, la Comisión y la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad determinará las acciones necesarias para dar una respuesta a escala de la UE a estas amenazas, basándose en la Estrategia de Ciberseguridad de la UE de 2013.

La protección de la privacidad y de los datos de carácter personal es un derecho fundamental y, por lo tanto, la piedra angular de cualquier acción encaminada a conseguir una auténtica Unión de la Seguridad. La Directiva sobre protección de datos en los ámbitos policial y penal adoptada en abril de 2016 garantiza una nivel común elevado

[1] La Comisión presentará en las próximas semanas un plan de acción revisado sobre los retornos; véase el informe de la Comisión al Parlamento Europeo, al Consejo Europeo y al Consejo sobre la puesta en marcha de la Guardia Europea de Fronteras y Costas [COM(2017) 42].

de protección de datos y, con ello, facilita el intercambio fluido de los datos oportunos entre las autoridades policiales y judiciales de los Estados miembros. La Comisión también ha iniciado una revisión de la Directiva sobre privacidad electrónica como parte de su «paquete en materia de datos» para ampliar el ámbito de aplicación de la Directiva a fin de incluir a todos los proveedores de servicios de comunicaciones electrónicas y adaptar sus disposiciones al Reglamento general de protección de datos. La propuesta tiene por objeto garantizar la protección de la privacidad de las comunicaciones electrónicas, exponiendo al mismo tiempo los motivos por los que se pueda restringir el alcance del Reglamento relativo a la privacidad electrónica, como, por ejemplo, motivos de seguridad nacional o investigaciones penales.

II. FORTALECER LOS SISTEMAS DE INFORMACIÓN Y LA INTEROPERABILIDAD

En el Discurso sobre el Estado de la Unión del presidente Juncker de septiembre de 2016 y las conclusiones del Consejo Europeo de diciembre de 2016 se señala la importancia de subsanar las deficiencias actuales de gestión de la información y de mejorar la **interoperabilidad y la interconexión entre los sistemas de información existentes**. Los hechos ocurridos recientemente han vuelto a llamar la atención sobre la urgente necesidad de vincular entre sí las bases de datos existentes en la UE, especialmente para dar a la policía de fronteras y los cuerpos y fuerzas de seguridad sobre el terreno los instrumentos necesarios para detectar la suplantación de identidad. Por ejemplo, el autor del atentado terrorista de Berlín de diciembre de 2016 empleó al menos catorce identidades diferentes y pudo pasar entre los Estados miembros sin ser detectado. Hay una evidente necesidad de que se puedan efectuar búsquedas de modo simultáneo en los sistemas de información existentes y futuros de la UE utilizando identificadores biométricos para cerrar esta vía a los terroristas y delincuentes.

A este respecto, en abril de 2016 la Comisión empezó a trabajar con sus propuestas relativas a unos «sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad»[2]. Se detectaron deficiencias en lo que respecta a las funcionalidades de los sistemas existentes, lagunas en la arquitectura de la UE de gestión de datos, problemas por la compleja diversidad de los sistemas de información regulados de manera diferente y una gran fragmentación ocasionada por el hecho de que los sistemas actuales se diseñaron de manera individual y no de manera interconectada. Como parte de este proceso, la Comisión creó el «**Grupo de Expertos de Alto Nivel sobre Sistemas de Información e Interoperabilidad**» con las agencias de la UE, los Estados miembros y las partes interesadas pertinentes. El 21 de diciembre de 2016[3], en un informe del presidente figuran las **conclusiones provisionales** del Grupo, que incluyen la opción prioritaria de crear un portal único de búsqueda para permitir que la policía de fronteras y los cuerpos y fuerzas de seguridad realicen búsquedas simultáneas en las bases de datos y sistemas de información de la UE existentes. El informe provisional destaca asimismo la importancia de la calidad de los datos, ya que los sistemas de información no tienen más eficacia que la de la calidad y el formato de los

[2] Comunicación «Sistemas de información más sólidos e inteligentes para la gestión de las fronteras y la seguridad» [COM(2016) 205 final].

[3] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=28994&no=1

datos consignados en ellos, y formula recomendaciones para aumentar la calidad de los datos en los sistemas de la UE gracias al control automatizado de la calidad de los datos.

En breve, la Comisión efectuará un seguimiento de la opción de crear un portal único de búsqueda y, junto con la Agencia Europea para la Gestión Operativa de Sistemas Informáticos de Gran Magnitud, eu-LISA, iniciará sus trabajos sobre un portal capaz de buscar simultáneamente en todos los sistemas de la UE existentes. Se prevé realizar un estudio al respecto para junio a más tardar, como base para diseñar y probar un prototipo del portal antes de que finalice el año. La Comisión considera que, de modo paralelo, Europol debe proseguir su labor sobre una interfaz de sistemas que, cuando estén consultando sus propios sistemas nacionales, permita a los agentes de primera línea de los Estados miembros consultar automáticamente las bases de datos de Europol de forma simultánea.

El trabajo relativo a la interoperabilidad de los sistemas de información tiene como objetivo superar la actual fragmentación de la arquitectura de la UE en materia de gestión de datos para el control y la seguridad en las fronteras y de fronteras, de gestión de datos y de seguridad conexas y los puntos ciegos conexos. Cuando las bases de datos utilicen un registro común de datos de identidad — tal y como se prevé en el Sistema propuesto de Entrada/Salida de la UE y el Sistema Europeo de Información y Autorización de Viajes (ETIAS) —, solo podrá inscribirse a una persona con una única identidad en las diferentes bases de datos, lo que impide la utilización de distintas identidades falsas. Como primer paso, de acuerdo con lo sugerido en las conclusiones provisionales del Grupo de Expertos de Alto Nivel, la Comisión ha pedido a eu-LISA que analice los aspectos técnicos y operativos de la aplicación de un servicio de correspondencias biométricas compartidas. Tal servicio permitirá efectuar búsquedas en diferentes bases de datos con los datos biométricos, lo que sacaría a la luz identidades falsas que utilice la persona de que se trate en otro sistema. Por otra parte, el Grupo de Expertos de Alto Nivel debe determinar ahora si es necesario, técnicamente viable y proporcionado ampliar el **registro común de datos de identidad** previsto para el Sistema de Entrada/Salida y ETIAS a otros sistemas. Además de los datos biométricos almacenados en el servicio de correspondencias biométricas, dicho registro común de datos de identidad incluiría también datos de identidad alfanuméricos. El Grupo deberá presentar sus conclusiones al respecto en su informe final al final del mes de abril de 2017 a más tardar.

Los hechos ocurridos recientemente en materia de seguridad ponen de relieve la necesidad de reexaminar la cuestión de la **puesta en común obligatoria de información** entre Estados miembros. La propuesta de la Comisión de diciembre de 2016 de consolidar el **Sistema de Información de Schengen** establece, por primera vez, la obligación de que los Estados miembros emitan alertas sobre personas relacionadas con actos de terrorismo. Es importante que los colegisladores trabajen ahora en favor de la rápida adopción de las medidas propuestas. La Comisión está dispuesta a examinar si debe introducirse la obligación de compartir información en lo que se refiere a otras bases de datos de la UE.

III. PROTEGER NUESTROS OBJETIVOS NO MILITARES FRENTE A ATENTADOS TERRORISTAS

El atentado de Berlín ha sido el más reciente perpetrado en la UE dirigido contra los denominados objetivos «no militares o indefensos», que normalmente son zonas civiles

donde las personas se reúnen en gran número (por ejemplo, espacios públicos, hospitales, escuelas, estadios deportivos, centros culturales, cafés y restaurantes, centros comerciales y nudos de transporte). Por su propia naturaleza, esos lugares son vulnerables y difíciles de proteger y también se caracterizan por la alta probabilidad de que haya un gran número de víctimas en caso de ataque. Por todas estas razones, los terroristas los prefieren. La amenaza de futuros ataques contra objetivos no militares, incluidos los medios de transporte, sigue siendo grande, como lo confirman las evaluaciones disponibles, incluido el informe de Europol sobre los cambios en el *modus operandi* del Daesh[4].

La Agenda Europea de Seguridad de 2015 y la Comunicación de 2016 relativa a la seguridad de la Unión pusieron de manifiesto la necesidad de seguir trabajando con objeto de mejorar la seguridad y el uso de herramientas y tecnología de detección innovadoras para la protección de los objetivos «no militares». La Comisión ha estado trabajando para apoyar y fomentar el intercambio de mejores prácticas entre los Estados miembros para el desarrollo de mejores instrumentos de prevención y respuesta ante los ataques a estos objetivos. Este trabajo ha dado como resultado manuales operativos y documentación orientativa. En la actualidad, la Comisión está desarrollando, en estrecha cooperación con expertos de los Estados miembros, un manual general sobre procedimientos y formularios en materia de seguridad aplicables a diferentes objetivos no militares (por ejemplo, centros comerciales, hospitales, actos deportivos y manifestaciones culturales). El objetivo es facilitar a principios de 2017 directrices de protección de los objetivos no militares para los Estados miembros, sobre la base de las mejores prácticas de los Estados miembros.

Paralelamente, en febrero la Comisión convocará el primer taller con las autoridades nacionales sobre protección de los objetivos no militares, con vistas a intercambiar información y desarrollar las mejores prácticas sobre la compleja cuestión de la protección de estos objetivos y la protección y seguridad públicas. Asimismo, la Comisión financia un proyecto piloto llevado a cabo por Bélgica, los Países Bajos y Luxemburgo en el marco del Fondo de Seguridad Interior para establecer un centro regional de excelencia para las intervenciones especiales de los cuerpos y fuerzas de seguridad, que ofrecerá formación a los agentes de policía, que suelen ser quienes primero responden en caso de atentado.

Responder a los ataques contra objetivos no militares es un componente fundamental de la labor de la Comisión en el ámbito de la protección civil. En diciembre, la Comisión anunció las acciones que tiene la intención de llevar a cabo con los Estados miembros para proteger a los ciudadanos de la UE y reducir las vulnerabilidades inmediatamente después de un atentado terrorista. Estas acciones reforzarán la coordinación entre todos los actores que intervienen en la gestión de las consecuencias de los ataques, y la Comisión se ha comprometido a apoyar los esfuerzos de los Estados miembros facilitando formación y ejercicios conjuntos y garantizando un diálogo permanente a través de los puntos focales existentes y de grupos de expertos. La Comisión apoyará también el desarrollo de módulos especializados de respuesta a los ataques terroristas en el marco del Mecanismo de Protección Civil de la Unión, así como iniciativas para compartir la experiencia adquirida y sensibilizar a la opinión pública.

---

[4] Europol, *Changes in modus operandi of Islamic State (IS) revisited*, noviembre de 2016 — Información Pública de Europol, disponible en: https://www.europol.europa.eu/publications-documents/changes-in-modus-operandi-of-islamic-state-revisited

Junto con los Estados miembros, la Comisión va a estudiar también qué apoyo podría prestar la UE para contribuir al desarrollo de la resiliencia y a una mayor seguridad en torno a posibles objetivos no militares. Asimismo, los Estados miembros podrían solicitar financiación del Banco Europeo de Inversiones (BEI) (incluido el Fondo Europeo para Inversiones Estratégicas), en consonancia con las políticas de la UE y del Grupo BEI. Todo proyecto estará sujeto a los procedimientos habituales de toma de decisiones establecidos en la legislación.

En lo que se refiere a los objetivos fáciles específicos en las zonas de transporte público, como las partes públicas de los aeropuertos o las estaciones de ferrocarril, en el taller de la Comisión realizado al respecto en noviembre de 2016 con una amplia gama de partes interesadas se subrayó la necesidad de mantener un equilibrio entre las necesidades de seguridad, la comodidad de los pasajeros y las operaciones de transporte. En las conclusiones se destaca la importancia de crear una cultura de la seguridad que abarque no solo a los empleados sino también a los pasajeros, así como la importancia de realizar evaluaciones de los riegos locales, como base para determinar las medidas de respuesta apropiadas, y la necesidad de mejorar la comunicación entre todas las partes implicadas.

IV. HACER FRENTE A LOS RETOS DE LAS AMENAZAS CIBERNÉTICAS

La ciberdelincuencia y los ciberataques son los principales retos a los que se enfrenta la Unión y donde la acción a nivel de la UE puede contribuir a reforzar nuestra resiliencia colectiva. Cada día, los incidentes de ciberseguridad perjudican gravemente la vida de las personas y provocan importantes daños económicos a la economía y las empresas europeas. Los ciberataques son un componente fundamental de las amenazas híbridas: coordinados de modo preciso con amenazas físicas, por ejemplo en relación con el terrorismo, pueden tener un impacto devastador. Los ciberataques también pueden contribuir a desestabilizar un país, o a poner en jaque a sus instituciones políticas y sus procesos democráticos fundamentales. Dado que cada vez dependemos más de las tecnologías en línea, nuestras infraestructuras esenciales (que van de los hospitales a las centrales nucleares) serán cada vez más vulnerables.

La estrategia de ciberseguridad de la UE de 2013 forma parte de la política principal de respuesta a los retos en materia de ciberseguridad. La medida central es la Directiva sobre Seguridad de las Redes y de la Información[5] (SRI), adoptada el pasado mes de julio. Dicha Directiva sienta las bases para mejorar la cooperación a nivel de la UE y la ciberresiliencia mediante el apoyo a la cooperación y el intercambio de información entre los Estados miembros y el fomento de la cooperación operativa en incidentes de ciberseguridad específicos y la comunicación mutua de información sobre riesgos. Para garantizar una aplicación coherente en los diferentes sectores y a través de las fronteras, la Comisión celebrará en febrero la primera reunión del Grupo de Cooperación SRI con los Estados miembros.

[5] Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

En abril de 2016, la Comisión y la Alta Representante adoptaron un marco común para la lucha contra las amenazas híbridas[6], que propuso 22 acciones operativas destinadas a sensibilizar, aumentar la resiliencia, responder mejor a las crisis e intensificar la cooperación entre la UE y la OTAN. Tal como lo ha solicitado el Consejo, la Comisión y la Alta Representante de la UE presentarán a más tardar en julio de 2017 un informe de evaluación de los avances realizados.

Por otra parte, la Comisión promueve y apoya la innovación tecnológica, entre otros modos utilizando los fondos de investigación de la UE para impulsar nuevas soluciones y crear nuevas tecnologías que puedan contribuir a reforzar nuestra resiliencia frente a los ciberataques (por ejemplo, proyectos de «seguridad desde el diseño»). El pasado verano, la Comisión puso en marcha una asociación privada de 1 800 millones EUR con la industria sobre ciberseguridad[7].

En el ámbito del transporte, la digitalización se está convirtiendo en un motor importante de la muy necesaria transformación del sistema actual de transporte. El rápido ritmo de la digitalización aporta muchos beneficios, pero también hace que el transporte resulte más vulnerable a los riesgos en materia de ciberseguridad o ciberprotección. Son numerosas las acciones emprendidas para atenuar la amenaza a distintos niveles, concretamente en el sector de la aviación, pero también en los sectores del transporte marítimo, fluvial, ferroviario y por carretera[8]. Queda pendiente la clarificación, armonización y complementación de las actividades de las diferentes partes interesadas que participan en la mejora de distintos aspectos de la resiliencia cibernética.

En un contexto más amplio, y habida cuenta de la rápida evolución de la naturaleza de la amenaza, en los próximos meses la Comisión y la Alta Representante de la UE determinarán las acciones necesarias para dar una respuesta eficaz a nivel de la UE a estas amenazas, sobre la base de la estrategia de ciberseguridad de la UE de 2013.

V. PROTEGER LOS DATOS DE CARÁCTER PERSONAL, CONTRIBUYENDO AL MISMO TIEMPO A LA EFICACIA DE LAS INVESTIGACIONES PENALES

La Directiva sobre protección de datos para el ámbito policial y de la justicia penal[9] es una pieza clave de la lucha contra el terrorismo y los delitos graves. Sobre la base de una

---

6 JOIN (2016) 18.

7 Anunciada en la Comunicación sobre ciberresiliencia de 2016 [COM(2016) 410 final].

8 Ejemplos de ello son las directrices internacionales, como las elaboradas por la Organización Marítima Internacional (OMI) o mediante una resolución de la OACI adoptada recientemente, con la iniciativa conjunta de la UE y de los EE.UU.; la notificación de incidentes de modo más reactivo que está elaborando actualmente la Agencia Europea de Seguridad Aérea, y la ciberseguridad mediante el diseño, aplicable a nuevos sistemas que se están creando actualmente, como el plan director de gestión del tráfico aéreo (Plan Maestro ATM) de la empresa común SESAR.

9 Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 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, y la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. La Directiva, vigente desde el 5 de mayo de 2016, debe ser transpuesta por los Estados miembros antes del 6 de mayo de 2018. La Comisión ha

norma de protección de datos común establecida en la Directiva, las autoridades policiales y judiciales de los Estados miembros podrán intercambiar fluidamente los datos pertinentes, al tiempo que los datos de las víctimas, los testigos y los sospechosos de delitos estarán debidamente protegidos.

Además, a fin de garantizar un elevado nivel de confidencialidad de las comunicaciones, tanto para las personas como para las empresas, y unas condiciones de competencia equitativas para todos los operadores del mercado, tal como se establece en la Estrategia para el Mercado Único Digital de abril de 2015, la Comisión adoptó el 11 de enero la propuesta de **Reglamento sobre privacidad electrónica** (que sustituye a la Directiva 2002/58/CE)[10]. Tal como ocurre con la Directiva actual, el Reglamento revisado sobre privacidad electrónica particulariza el Reglamento general de protección de datos[11] y establece un marco que rige la protección de la privacidad y de los datos de carácter personal en el sector de las comunicaciones electrónicas.

Por medio de esta revisión, todos los datos de las comunicaciones electrónicas, aun cuando la comunicación sea accesoria, se considerarán confidenciales/restringidos, ya se realice a través de los servicios de telecomunicaciones tradicionales o de los servicios de transmisión libre (*over the top* - OTT) que, funcionalmente, son equivalentes (por ejemplo, *skype* y *whatsapp*) y, a menudo, para muchos usuarios son intercambiables con los operadores habituales de telecomunicaciones[12]. Las obligaciones impuestas a los proveedores de servicios, además de respetar las opciones de privacidad de sus clientes a la hora de utilizar, almacenar o procesar sus datos, también incluyen la obligación de los prestadores de servicios establecidos fuera de la UE de designar un representante en un Estado miembro. Ello dará también a los Estados miembros la posibilidad de facilitar la cooperación de las autoridades policiales y judiciales con los proveedores de servicios para acceder a las pruebas electrónicas (véase más adelante).

Al igual que con arreglo a las normas actuales en materia de privacidad electrónica, el acceso de las autoridades policiales y judiciales a la información electrónica pertinente y necesaria para la investigación de los delitos se regirá por la excepción establecida en el artículo 11 de la propuesta de Reglamento sobre la privacidad electrónica[13]. Esta disposición da la posibilidad, en el Derecho de la UE o el Derecho nacional, de restringir, en la legislación de la UE o la legislación nacional, la confidencialidad de la comunicación cuando sea necesario y proporcionado, con objeto de salvaguardar la seguridad nacional, la defensa, la seguridad pública y la prevención, la investigación, la

---

creado un grupo de expertos con los Estados miembros para intercambiar puntos de vista sobre la transposición de la Directiva relativa a la policía.

10 Reglamento sobre la privacidad y las comunicaciones electrónicas [COM(2017) 10].

11 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), que será aplicable el 25 de mayo de 2018.

12 Con ello se sigue el planteamiento adoptado en la propuesta de Directiva por la que se establece el Código Europeo de las Comunicaciones Electrónicas, presentada por la Comisión el 14 de septiembre de 2016 (paquete de telecomunicaciones) [COM(2016) 590 final].

13 Véase el artículo 11, apartado 1, «cláusula de conservación de datos», que no ha variado respecto al artículo 15 de la Directiva de privacidad electrónica y es conforme a los requisitos del Reglamento general sobre protección de datos. Dicha limitación debe respetar la esencia de los derechos fundamentales y ser necesaria, adecuada y proporcionada.

detección o la persecución de delitos penales o la aplicación de sanciones penales. Esta disposición es especialmente pertinente para las normas nacionales de **conservación de datos**, es decir, para obligar a los proveedores de servicios de telecomunicaciones a conservar los datos de las comunicaciones durante un período de tiempo determinado para su acceso, en su caso, a efectos policiales o judiciales, a raíz de la decisión del Tribunal de Justicia de la Unión Europea (TJUE) de anulación de la Directiva sobre conservación de datos en 2014[14]. Desde entonces, no ha habido ningún instrumento de la UE sobre conservación de datos, y algunos Estados miembros han adoptado sus propias legislaciones nacionales de conservación de datos. Las leyes de conservación de datos de Suecia y el Reino Unido fueron impugnadas ante el Tribunal de Justicia, que dictó su sentencia *Tele2* el 21 de diciembre[15]. El TJUE consideró incompatible con el Derecho de la Unión una normativa nacional que, para luchar contra la delincuencia, establece una conservación general e indiscriminada de todos los datos de tráfico y localización de los abonados y usuarios en todos los medios de comunicación electrónicos. Las implicaciones de la sentencia se están analizando, y la Comisión preparará orientaciones sobre cómo puede elaborarse legislación nacional sobre conservación de datos de conformidad con la sentencia.

La delincuencia deja rastros digitales que pueden servir como medio de prueba en procesos judiciales; las comunicaciones electrónicas entre sospechosos suelen ser a menudo la única pista que pueden obtener las autoridades policiales y judiciales. Sin embargo, conseguir el acceso a **pruebas electrónicas**, especialmente si se hallan en el extranjero o en una nube, puede ser complejo, tanto desde un punto de vista técnico como jurídico, y es a menudo gravoso desde el punto de vista procesal, lo que impide que los investigadores avancen rápidamente. Para abordar estos retos, la Comisión está estudiando actualmente soluciones para que los investigadores puedan obtener pruebas electrónicas transfronterizas, que incluyan una asistencia jurídica mutua más eficiente y la búsqueda de modos de cooperación directa con los proveedores de servicios de internet, y proponer criterios para determinar y ejecutar la competencia judicial en el ciberespacio, respetando plenamente las normas de protección de datos aplicables[16]. El 9 de diciembre de 2016, la Comisión informó al Consejo de Justicia y Asuntos de Interior sobre los progresos realizados[17].

Un proceso de consulta de expertos global (todavía en curso) ha permitido a la Comisión definir los distintos y a menudo complejos problemas suscitados por el acceso a las pruebas electrónicas, tener un mayor conocimiento de las actuales normas y prácticas en los Estados miembros e identificar posibles opciones estratégicas. El informe de situación proporciona un panorama de las ideas que han surgido hasta ahora durante la recopilación de información y el proceso de consulta de expertos y que la Comisión, en consulta con las partes interesadas, examinará más detalladamente en los próximos

[14] Sentencia del TJUE en los asuntos acumulados C-293/12 y C-594/12, Digital Rights Ireland, de 8 de abril de 2014.

[15] Sentencia del TJUE en los asuntos acumulados C−203/15 y C−698/15, Tele2, de 21 de diciembre de 2016.

[16] Con arreglo al compromiso asumido en la Agenda Europea de Seguridad, [COM(2015) 185 final], y la Comunicación de la Comisión titulada «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].

[17] En sus conclusiones sobre la mejora de la justicia penal en el ciberespacio, de 9 de junio de 2016, el Consejo invitó a la Comisión a adoptar medidas concretas, desarrollar un enfoque común de la UE y presentar resultados a más tardar en junio de 2017.

meses. Como se anunció en el programa de trabajo de la Comisión, esta presentará una iniciativa en 2017.

VI. CONCLUSIÓN

El próximo informe, que debe presentarse el 1 de marzo, brindará una oportunidad para pasar revista a los avances conseguidos en la aplicación de estas y otras líneas principales de trabajo.