Consejo de la Unión Europea

Bruselas, 2 de octubre de 2017
(OR. en)

12711/17

GENVAL 79
CYBER 136
CATS 98
JAI 855

NOTA PUNTO «I/A»

De:	Secretaría General del Consejo
A:	Comité de Representantes Permanentes/Consejo
N.º doc. prec.:	9986/2/17 REV 2
Asunto:	Informe definitivo de la séptima ronda de evaluaciones mutuas sobre la «Aplicación práctica y funcionamiento de las políticas europeas de prevención y lucha contra la ciberdelincuencia» - Información al Consejo

De conformidad con el artículo 2 de la Acción Común 97/827/JAI de 5 de diciembre de 1997[1], el Grupo «Cuestiones Generales, incluida la Evaluación» (GENVAL) decidió, el 3 de octubre de 2013, que la séptima ronda de evaluaciones mutuas se dedicaría a la aplicación práctica y al funcionamiento de las políticas europeas de prevención y lucha contra la ciberdelincuencia.

[1] Acción Común 97/827/JAI, de 5 de diciembre de 1997, adoptada por el Consejo sobre la base del artículo K.3 del Tratado de la Unión Europea, por la que se establece un mecanismo de evaluación de la aplicación y ejecución a escala nacional de los compromisos internacionales en materia de lucha contra la delincuencia organizada (DO L 344 de 15.12.1997).

El proyecto de informe final que recoge el documento 9986/17, que ha sido elaborado por la Secretaría General del Consejo e incluye las conclusiones y recomendaciones contenidas en los informes adoptados con anterioridad para cada Estado miembro, se presentó al Grupo GENVAL, en su reunión del 13 de junio de 2017, con vistas a un intercambio preliminar de puntos de vista.

Se pidió a las delegaciones que presentaran por escrito sus observaciones sobre el proyecto de informe definitivo a más tardar el 3 de julio de 2017.
La versión revisada del informe, que figura en el documento 9986/17 REV 1, fue presentada al Grupo Horizontal «Cuestiones Cibernéticas» en su reunión del 4 de septiembre de 2017.

A raíz de los comentarios de una delegación, el proyecto de informe se ha revisado ligeramente, tal como se recoge en el anexo del documento 9986/2/17 REV 2, y fue refrendado por el CATS en su reunión del 22 de septiembre de 2017. Posteriormente, en la versión final del informe que figura en el anexo se introdujeron algunos cambios de redacción, pocos y de escasa importancia.

Se invita al Coreper a que presente a título informativo al Consejo, para que este tome nota de los resultados de la evaluación, el informe final de la séptima ronda de evaluaciones mutuas recogido en el anexo.

De conformidad con el artículo 8, apartado 4, de la mencionada Acción Común, el informe definitivo deberá remitirse también al Parlamento Europeo a título informativo.

ANEXO

Informe final sobre la séptima ronda de evaluaciones mutuas sobre «Aplicación práctica y funcionamiento de las políticas europeas de prevención y lucha contra la ciberdelincuencia»

ÍNDICE

I. INTRODUCCIÓN

A raíz de la adopción de la Acción común 97/827/JAI, de 5 de diciembre de 1997, por la que se establece un mecanismo de evaluación de la aplicación y ejecución a escala nacional de los compromisos internacionales en materia de lucha contra la delincuencia organizada, el presente informe trata de resumir las conclusiones y recomendaciones y de establecer conclusiones en lo que respecta a la séptima ronda de evaluación mutua.

De conformidad con el artículo 2 de la mencionada Acción Común, el Grupo «Cuestiones Generales, incluida la Evaluación» (GENVAL) decidió, el 3 de octubre de 2013, que la séptima ronda de evaluaciones mutuas se dedicaría a la aplicación práctica y al funcionamiento de las políticas europeas de prevención y lucha contra la ciberdelincuencia.

La elección de la ciberdelincuencia como tema de la séptima ronda de evaluaciones mutuas fue muy bien acogida por los Estados miembros. Sin embargo, en vista de la amplia gama de delitos que abarca el término «ciberdelincuencia», se acordó que la evaluación se centraría en los delitos que, según los Estados miembros, requerían especial atención. A tal fin, la evaluación se ha referido a: los ataques cibernéticos, el abuso sexual de menores, la pornografía infantil en línea y el fraude en línea con tarjetas de pago, y ha ofrecido un examen exhaustivo de los aspectos jurídicos y prácticos de la lucha contra la ciberdelincuencia, la cooperación transfronteriza y la cooperación con los organismos pertinentes de la UE. A este respecto, son especialmente pertinentes la Directiva 2011/92/UE, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil[2] (fin de plazo de incorporación al Derecho nacional: 18 de diciembre de 2013) y la Directiva 2013/40/UE[3] relativa a los ataques contra los sistemas de información (fin de plazo de incorporación al Derecho nacional: 4 de septiembre de 2015).

[2] DO L 335 de 17.12.2011, p. 1.
[3] DO L 218 de 14.8.2013, p. 8.

El cuestionario para la séptima ronda de evaluaciones mutuas fue examinado por GENVAL los días 27 de noviembre de 2013 y 22 de enero de 2014 y posteriormente fue adoptado mediante procedimiento tácito el 31 de enero de 2014. El orden de visitas, sin prejuicio de ciertos ajustes, y la composición de los equipos de evaluación relacionada con los observadores fueron aprobados por GENVAL el 1 de abril de 2014.

De conformidad con el artículo 3 de la Acción Común 97/827/JAI, los Estados miembros designaron expertos con conocimientos prácticos sustanciales en la materia, previa petición escrita dirigida a las delegaciones por el jefe de la Unidad DGD 2B de la Secretaría General del Consejo el 28 de enero de 2014. En cada misión participaron tres expertos nacionales en la evaluación. Otros expertos, de la Comisión, Eurojust, Europol y ENISA participaron en algunas misiones de evaluación en calidad de observadores. La Secretaría General del Consejo coordinó y participó en las misiones con uno o dos miembros de su personal para cada evaluación, preparó el proceso y ayudó a los expertos.

La primera misión de evaluación se llevó a cabo en Francia entre el 28 y el 31 de octubre de 2014. La misión final de evaluación tuvo lugar en Suecia entre el 27 y el 30 de septiembre de 2016. Las veintiocho misiones de evaluación han dado lugar a informes detallados sobre cada uno de los Estados miembros. Estos informes de evaluación han sido ulteriormente debatidos y adoptados en el Grupo GENVAL[4]. La mayoría de estos informes está disponible en el sitio web del Consejo y son accesibles públicamente.

[4] Francia (7588/2/15 REV 1 DCL 1); Países Bajos (7587/15 DCL 1); Reino Unido (10952/2/15 REV 2 DCL 1); Rumanía (13022/1/15 REV 1 DCL 1); Eslovaquia (9761/1/15 REV 1 DCL 1). Estonia (10953/15 DCL 1); Eslovenia (14586/1/16 REV 1 DCL 1); Italia (9955/1/16 REV 1 DCL 1); España (6289/1/16 REV 1 DCL 1); Bulgaria (5156/1/16 REV 1 DCL 1); Lituania (6520/1/16 REV 1 DCL 1); Malta (7696/1/16 REV 1 DCL 1); Grecia (14584/1/16 REV 1 DCL 1); Croacia (5250/1/17 REV 1 DCL 1); Portugal (10905/1/16 REV 1 DCL 1); Chipre (9892/1/16 REV 1 DCL 1); Polonia (14585/1/16 REV 1 DCL 1); República Checa (13203/1/16 REV 1 DCL 1); Hungría (14583/1/16 REV 1 DCL 1); Letonia (5387/1/17 REV 1 DCL 1); Dinamarca (13204/1/16 REV 1 DCL 1 + COR 1); Bélgica (8212/1/17 REV 1); Austria (8185/1/17 REV 1); Alemania (7159/1/17 REV 1 DCL 1); Luxemburgo (7162/1/17 REV 1 DCL 1); Irlanda (7160/1/17 REV 1 DCL 1); Finlandia (8178/17); Suecia (8188/17 REV 1).

El presente documento incluye las conclusiones y recomendaciones contenidas en informes específicos elaborados anteriormente respecto de cada Estado miembro[5]. No obstante, cabe señalar que, debido al carácter dilatado de la evaluación, los distintos informes pueden no reflejar íntegramente el estado actual de la situación.

[5] Los distintos informes se redactaron justo después de la visita a los Estados miembros. Con posterioridad a esta visita pueden haberse producido cambios que no se reflejan en los distintos informes, por ejemplo el término de la aplicación de la legislación. El seguimiento de los informes de evaluación, previsto dieciocho meses a partir de la adopción, debería reflejar las modificaciones introducidas. En el momento de debatir el informe en el Grupo GENVAL, los Estados miembros anunciaron a menudo (futuros) cambios para seguir las recomendaciones formuladas en su informe individual.

II- SÍNTESIS

- Como consecuencia del uso más frecuente de Internet, la ciberdelincuencia es un fenómeno delictivo en expansión, y están surgiendo nuevas tendencias y *modus operandi*, tanto en la ciberdelincuencia en sentido estricto, que se define jurídicamente como aquellos delitos que requieren la presencia de un sistema informático, como en los delitos favorecidos por el ámbito cibernético, que son delitos tradicionales cometidos utilizando tecnología de la información y de la comunicación (TIC). Por lo tanto, en todos los países, avanzar en la lucha contra la ciberdelincuencia exige un alto nivel de voluntad política, esfuerzos presupuestarios y una inversión importante en recursos humanos y técnicos.

- La evaluación ha evidenciado que todos los Estados miembros se toman en serio la lucha contra la ciberdelincuencia y que disponen de estructuras, recursos y medidas a tal fin. Sin embargo, el grado de compromiso y eficacia varía en los Estados miembros y en algunos casos todavía cabe mejorar en relación con determinados aspectos del planteamiento global para combatir la ciberdelincuencia. Al mismo tiempo también se han identificado algunos problemas y retos comunes.

- En el momento de la evaluación, la mayoría de los Estados miembros había adoptado una estrategia nacional de seguridad cibernética, que proporciona un marco para establecer las prioridades nacionales, así como las principales estructuras de coordinación a nivel estratégico y operativo para luchar contra la ciberdelincuencia y garantizar la resiliencia cibernética, mientras que un número reducido de Estados miembros estaba a punto de hacerlo. Algunos Estados Miembros también habían adoptado un plan de acción para la aplicación de su estrategia nacional de seguridad cibernética.

- En el momento de la evaluación, la mayoría de los Estados miembros había firmado y ratificado el Convenio de Budapest sobre la Ciberdelincuencia (Consejo de Europa, 2001) y gran parte de ellos también su Protocolo adicional sobre la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos. Se ha exhortado a los Estados miembros que aún no lo hayan hecho a que firmen y ratifiquen estos instrumentos.

- Una de las principales deficiencias detectadas se refiere a la recogida de estadísticas independientes sobre ciberdelincuencia y seguridad cibernética, ya que las disponibles son insuficientes y fragmentarias, y no permiten ni la comparación entre las diferentes regiones de un mismo Estado miembro ni entre los diferentes Estados miembros. Es necesario disponer de estadísticas fiables para tener una visión de conjunto, supervisar y analizar las tendencias y la evolución de la ciberdelincuencia, con vistas a tomar las medidas oportunas y a evaluar la eficacia del sistema jurídico para contrarrestar esta forma de delincuencia. Por consiguiente, se ha recomendado a los Estados miembros que recopilen estadísticas específicas y completas sobre la ciberdelincuencia en las distintas fases del procedimiento siguiendo un enfoque normalizado.

- Debido al rápido desarrollo de las TIC con métodos cada vez más sofisticados, y dada la complejidad de la ciberdelincuencia, es sumamente importante un alto grado de especialización de los profesionales que trabajen en este ámbito. Según las conclusiones de la evaluación, el nivel de especialización es generalmente suficiente o satisfactorio en lo que respecta a los cuerpos y fuerzas de seguridad, mientras que hay margen de mejora en lo que se refiere al ámbito judicial, dado que en varios Estados miembros se ocupan de la ciberdelincuencia las fiscalías generales y los tribunales penales generales. Por consiguiente, se ha recomendado a los Estados miembros que aumenten el nivel de especialización de su personal judicial encargado de los casos de ciberdelincuencia.

- Por las mismas razones, la evaluación ha puesto de manifiesto la importancia de que se imparta una formación especializada periódica y continua sobre ciberdelincuencia tanto para los cuerpos y fuerzas de seguridad como para el poder judicial, en particular haciendo un mejor uso de las posibilidades de formación que ofrecen o a las que contribuyen, según sus mandatos, organismos de la UE como EC3/Europol, ECTEG, Eurojust, OLAF y CEPOL.

- La evaluación ha puesto de relieve que una coordinación y una cooperación interinstitucional estrechas y eficaces basadas en un enfoque multiinstitucional a nivel estratégico y operativo entre todas las partes interesadas públicas y privadas que intervienen en la ciberdelincuencia y la seguridad cibernética constituyen un elemento clave para luchar de manera eficaz contra la ciberdelincuencia y garantizar un buen nivel de resiliencia de los sistemas nacionales de seguridad cibernética contra las amenazas cibernéticas. Sin embargo, en algunos Estados miembros esta cooperación no ha sido suficientemente desarrollada o puede mejorarse aún más.

- Para ello, también se ha exhortado a los Estados miembros a que consideren la posible creación de un organismo/entidad central en el que estén representados tanto el sector público como el privado para coordinar las actividades en este ámbito.

- En este contexto es crucial una estrecha cooperación entre el sector público y el sector privado, las entidades financieras/bancarias, las compañías de telecomunicaciones, los proveedores de servicios de Internet, las ONG, las asociaciones académicas, empresariales y profesionales, etc., ya que su experiencia posee un gran valor añadido para el éxito de las investigaciones en materia de ciberdelincuencia y de las acciones emprendidas para responder a los incidentes cibernéticos. Las formas más avanzadas de cooperación con el sector privado se institucionalizan mediante la creación de autoridades/grupos de trabajo adecuados. Las asociaciones público-privadas han sido identificadas por los evaluadores como una herramienta importante para una buena cooperación entre los cuerpos y fuerzas de seguridad y el sector privado.

- Algunos Estados miembros mantienen contactos directos con los proveedores de servicios de Internet ubicados en el extranjero, especialmente en Estados Unidos, pero el resultado de las peticiones que se cursan es a menudo incierto debido al carácter voluntario de la cooperación; por tanto, beneficiaría a la UE y a los Estados miembros que se definiesen normas claras que establezcan la manera en que los cuerpos y fuerzas de seguridad pueden obtener datos de los proveedores de servicios de Internet extranjeros.

- En algunos Estados miembros la legislación nacional permite obtener información básica sobre los abonados directamente de los proveedores de servicios extranjeros, mientras que en otros es necesario seguir los procedimientos de asistencia judicial, los cuales deberían ser más rápidos y efectivos. Se ha instado a los Estados miembros a que velen por que su normativa nacional sea suficientemente flexible como para facilitar la admisibilidad de pruebas electrónicas, también en los casos en que se hayan obtenido en otro país o directamente de los proveedores de servicios.

- El creciente uso de cifrado con técnicas cada vez más sofisticadas se está convirtiendo en un reto cada vez mayor para las fuerzas del orden y las autoridades de inteligencia en todos los Estados miembros, ya que dificulta o impide totalmente acceder a información pertinente sobre ciberdelincuencia. El descifrado puede ser posible –si acaso– mediante la utilización de material y programas informáticos especializados de gran capacidad, y la evaluación ha puesto de manifiesto que los resultados no han sido muy alentadores a la hora de tratar un cifrado sin fallos. Muchos Estados miembros hacen uso de la plataforma de descifrado de Europol en el Centro Europeo de Ciberdelincuencia (EC3). Según los resultados de la evaluación, los desafíos planteados por el cifrado podrían compensarse parcialmente intensificando la investigación y el desarrollo, y elaborando nuevos métodos, así como mediante una buena cooperación entre las distintas autoridades implicadas. Se ha recomendado también a los Estados miembros y a las instituciones de la UE que estudien soluciones e intensifiquen un diálogo abierto con el sector privado.

- La naturaleza de las pruebas electrónicas puede crear, en lo que respecta a su admisibilidad, problemas que no se dan con otros tipos de pruebas. Por esta razón, en algunos Estados miembros existen requisitos específicos en lo que respecta a la recopilación de pruebas electrónicas para que sean admisibles en los tribunales. Sin embargo, la evaluación ha puesto de manifiesto que en la mayoría de los Estados miembros, el Derecho procesal es esencialmente neutro desde el punto de vista tecnológico, lo que significa que se aplican normas y principios generales sobre la obtención de pruebas y que el sistema procesal no contiene normas formales específicas sobre admisibilidad y evaluación de las pruebas electrónicas.

- La evaluación ha revelado que la ciberdelincuencia con datos almacenados en la «nube» plantea en general problemas para la investigación y el procesamiento, dado que la información en la «nube» es de difícil localización y acceso para los cuerpos y fuerzas de seguridad. Según cada caso concreto, la prueba electrónica puede localizarse en jurisdicciones de uno o varios Estados miembros, incluso fuera de la UE simultáneamente. Por lo tanto, pueden surgir conflictos de jurisdicción; en estas circunstancias se puede solicitar la asistencia de Eurojust y de la RJE. La evaluación ha puesto de relieve la importancia de que se aborden estos retos a nivel de la UE e internacional.

- La evaluación ha confirmado las preocupaciones de los Estados miembros en relación con la ausencia de un marco jurídico común en materia de conservación de datos a nivel de la UE. Este hecho repercute en la eficacia de las investigaciones y los procedimientos penales, sobre todo cuando se trata de recopilar datos de comunicaciones electrónicas para utilizarlos como pruebas ante los tribunales, así como en la cooperación judicial transfronteriza. La evaluación hace hincapié en la necesidad de un enfoque común a nivel de la UE. Actualmente se está llevando a cabo un proceso de reflexión común entre las instituciones de la UE y los Estados miembros para abordar la cuestión de la conservación de los datos con el fin de definir soluciones jurídicas y prácticas a los retos derivados de la jurisprudencia del Tribunal de Justicia.

- El abuso sexual de menores en Internet, en sus distintas formas, ha aumentado de manera significativa en los últimos años. A fin de combatir eficazmente estas formas de delincuencia, se aplica en distinta medida en los Estados miembros una amplia gama de medidas preventivas (por ejemplo, campañas de formación e información destinadas a sensibilizar a la opinión pública) y de medidas coercitivas (bloqueo del acceso o eliminación de contenidos ilegales), con la participación tanto del sector público como del privado. La evaluación ha evidenciado que únicamente algunos Estados miembros cuentan con una base de datos nacional dedicada a la identificación de las víctimas para luchar contra el abuso sexual de menores; a los demás Estados miembros que únicamente utilizan la Base de Datos Internacional sobre Explotación Sexual de Niños de Interpol (ICSE-DB), se les ha recomendado que desarrollen una base de datos nacional de este tipo. Varios Estados miembros han adoptado medidas destinadas a prevenir la revictimización de menores, incluso en algunos casos para proteger a las víctimas y testigos de abusos sexuales a niños durante los procesos penales. Se ha determinado que una buena cooperación entre todas las partes interesadas pertinentes, a saber, las los cuerpos y fuerzas de seguridad, las líneas directas, las ONG y los proveedores de servicios de Internet constituye un elemento esencial para combatir esta forma de delincuencia.

- En lo que respecta a la seguridad cibernética, los equipos nacionales de respuesta a emergencias informáticas que la mayoría de Estados miembros ya ha establecido desempeñan un papel crucial en el control y la respuesta a los incidentes cibernéticos. Además, los Estados miembros incorporarán en su legislación nacional la obligación para los operadores de servicios esenciales de notificar sin demora, a las autoridades competentes de los equipos nacionales de respuesta a emergencias informáticas, los incidentes cibernéticos que tengan efectos importantes en la continuidad de los servicios esenciales. Ambas cuestiones están previstas por la Directiva SRI y deberán aplicarse a más tardar el 9 de mayo de 2018.

- Como en las investigaciones sobre la ciberdelincuencia en sentido estricto y sobre la delincuencia favorecida por el ámbito cibernético interviene con frecuencia más de un Estado miembro, es prioritario cooperar e intercambiar información con los organismos de la UE (Europol/EC3, Eurojust, la RJE y ENISA), y que estos lo hagan si procede. Por la misma razón, se ha recomendado un uso más amplio de los equipos conjuntos de investigación (ECI), como instrumento eficaz para llevar a cabo investigaciones transfronterizas.

- Internet no tiene fronteras y, por lo tanto, una cooperación internacional fluida y eficaz es crucial para luchar eficazmente contra la ciberdelincuencia. Sin embargo, como se pone de manifiesto en la evaluación, los procedimientos de asistencia judicial suelen ser lentos, premiosos e ineficaces, y ello tiene un impacto negativo en las investigaciones, mientras que lo que se necesita es obtener con rapidez las pruebas electrónicas debido a su volatilidad. En consecuencia, es necesario acelerar la tramitación de las solicitudes de asistencia judicial en las investigaciones de los ciberdelitos. Además, se ha exhortado a los Estados miembros a que utilicen con más frecuencia los instrumentos de Eurojust, la Red Judicial Europea y Europol, y

III - ESTRATEGIA NACIONAL DE SEGURIDAD CIBERNÉTICA

CONCLUSIONES Y RECOMENDACIONES CLAVE

- En el momento de la evaluación, la mayoría de los Estados miembros había adoptado una estrategia nacional de seguridad cibernética, y algunos de ellas también un plan de acción para su aplicación, mientras que un numero reducido de Estados miembros estaba en proceso de hacerlo.

- Tras el desarrollo de una estrategia nacional de seguridad cibernética y, en su caso, de un plan de acción, es esencial garantizar un seguimiento adecuado y supervisar estrechamente la ejecución de la estrategia nacional.

- Debido al rápido desarrollo tanto de la TIC como de los nuevos tipos de delitos relacionados con el ámbito cibernético, también es necesario actualizar constantemente las medidas y los medios establecidos para combatir eficazmente la ciberdelincuencia y, por consiguiente, para garantizar, cuando sea necesario, la oportuna revisión de la estrategia nacional de seguridad cibernética.

- La creación de un organismo único con funciones de coordinación para la aplicación de la estrategia nacional de seguridad cibernética, como en algunos Estados miembros, puede considerarse una buena práctica que deberían seguir otros Estados miembros.

- La adopción de una estrategia nacional de seguridad de las redes y sistemas de información está prevista en la recientemente adoptada Directiva 2016/1148/ (Directiva SRI), para definir los objetivos estratégicos y las medidas estratégicas y reglamentarias apropiadas con objeto de alcanzar y mantener un elevado nivel de seguridad de las redes y de los sistemas de información (artículo 7).

RECOMENDACIONES
• ***Se exhorta a los Estados Miembros que aún no hayan adoptado una estrategia nacional de seguridad cibernética a que lo hagan lo antes posible y a que consideren asimismo la adopción de un plan de acción; aquellos que la hayan adoptado deben velar por su correcta aplicación y por la posible atribución a un único organismo/entidad de funciones de coordinación a tal fin.***
• ***Los Estados miembros deben actualizar su estrategia nacional de seguridad cibernética siempre que sea necesario, en consonancia con la evolución de la TIC pertinente, así como con las tendencias en la esfera de la ciberdelincuencia.***

IV - CONVENIO DE BUDAPEST

CONCLUSIONES Y RECOMENDACIONES CLAVE

- El Convenio de Budapest sobre la Ciberdelincuencia (Consejo de Europa, 2001) es el primer y único tratado internacional concebido para lograr una política penal común que garantice la protección de la sociedad contra la ciberdelincuencia, especialmente mediante la adopción de una legislación adecuada y el fomento de la cooperación internacional.

- En el Convenio de Budapest se definen los delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos, la falsificación informática y el fraude informático, la pornografía infantil y las infracciones de la propiedad intelectual.

- También prevé una serie de competencias y procedimientos, como la conservación y revelación rápida de datos, las órdenes de presentación, la búsqueda de las redes informáticas y la interceptación legal.

- El artículo 35 establece la red internacional 24/7 de asistencia inmediata a efectos de investigaciones o procedimientos, que permite congelar los datos, permitiendo así que se conserven las pruebas electrónicas. Este último es un instrumento importante, ya que crea una posibilidad rápida de preservación de pruebas electrónicas antes de enviar una solicitud de asistencia judicial.

- El Convenio de Budapest se completó mediante un Protocolo adicional relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos y, por lo que se refiere a la protección de los niños contra la explotación y el abuso sexual, mediante el Convenio de Lanzarote.
- En el momento de la evaluación, la mayoría de los Estados miembros había firmado y ratificado estos instrumentos, aunque unos pocos todavía no lo habían hecho. En las Conclusiones del Consejo de 9 de junio de 2016 sobre la mejora de la justicia penal en el ciberespacio se reiteraba el llamamiento a que los Estados miembros que todavía no lo habían hecho ratificasen y aplicasen plenamente el Convenio sobre la Ciberdelincuencia y su Protocolo adicional.

RECOMENDACIONES
• ***Se exhorta a los Estados Miembros que aún no lo hayan hecho a que firmen y ratifiquen el Convenio de Budapest sobre la Ciberdelincuencia (Consejo de Europa, 2001) y su Protocolo adicional, y a que apliquen plenamente estos instrumentos.***

V- ESTADÍSTICAS

CONCLUSIONES Y RECOMENDACIONES CLAVE

- El análisis de la legislación de la UE evidencia una clara necesidad de que se recopilen estadísticas en el ámbito de la ciberdelincuencia. De conformidad con el artículo 14, apartado 1, de la Directiva 2013/40/UE relativa a los ataques contra los sistemas de información, los Estados miembros garantizarán el establecimiento de un sistema para la recogida, elaboración y suministro de datos estadísticos sobre las infracciones mencionadas en los artículos 3 a 7.

- De conformidad con el artículo 14, apartado 2, de dicha Directiva, los datos estadísticos mencionados en el apartado 1 se referirán, como mínimo, a los datos existentes sobre el número de infracciones mencionadas en los artículos 3 a 7 que han sido registrados por los Estados miembros y al número de personas procesadas y condenadas por las infracciones mencionadas en los artículos 3 a 7.

- Además, de conformidad con el considerando 44 de la Directiva 2011/93/UE, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil, se alienta a los Estados miembros a crear mecanismos para la recogida de datos, o puntos de información, a nivel nacional o local y en colaboración con la sociedad civil, con objeto de observar y evaluar el fenómeno de los abusos sexuales y la explotación sexual de los menores.

- Por otra parte, la necesidad de recopilar estadísticas a escala nacional se desprende *in principio* en los Estados miembros de su legislación o normas nacionales.

- Las estadísticas sobre ciberdelincuencia son sumamente importantes. Por una parte, permiten un análisis y una comprensión detallados de la magnitud de las nuevas tendencias emergentes de esta forma de delincuencia en expansión, posibilitando de este modo que se disponga de una imagen realista del índice de ciberdelincuencia, debido a la escasa notificación de tales delitos, y que se siga su evolución, con miras a adoptar las medidas adecuadas; por otra parte, permiten evaluar la eficacia del sistema jurídico y de la adecuación de la legislación en la lucha contra la ciberdelincuencia y la protección de los intereses de los ciudadanos que son víctimas de estos delitos.

- Las estadísticas completas deben abarcar todas las fases del proceso: investigación, procesamiento, juicio, indicación del tipo de delito y medida específica de investigación, número de denuncias comunicado, número de investigaciones realizadas y las decisiones de no investigar determinados tipos de ciberdelincuencia, el número de víctimas y de denuncias de las víctimas, el número de personas procesadas y condenadas por diferentes tipos de ciberdelincuencia, el número de casos transfronterizos, el resultado de las solicitudes de asistencia judicial y la duración del procedimiento.

- Sin embargo, una de las principales deficiencias detectadas en la séptima ronda de evaluación en la mayoría de los Estados miembros está relacionada con la recogida de estadísticas diferenciadas sobre ciberdelincuencia en sentido estricto, delincuencia favorecida por el ámbito cibernético e incidentes de seguridad cibernética. Las existentes son insuficientes, fragmentarias y resultan incomparables en la mayoría de los Estados miembros.

- Además, muchos Estados miembros carecen de una definición nacional de la ciberdelincuencia en sentido estricto y de los delitos favorecidos por el ámbito cibernético a efectos estadísticos. En muchos Estados miembros, no es posible identificar la proporción de ciberdelincuencia en el cuadro de la delincuencia en general, y otros Estados miembros que recopilan estadísticas específicas sobre ciberdelincuencia las generan como un dato único; por consiguiente, no es posible clasificarlas en categorías ni distinguir entre los casos que se refieren a la ciberdelincuencia en sentido estricto y los que se refieren a los delitos favorecidos por el ámbito cibernético. No todos los Estados miembros presentan informes estadísticos periódicos sobre ciberdelincuencia.

- En la mayoría de los Estados miembros, las estadísticas judiciales están separadas de las estadísticas de los cuerpos y fuerzas de seguridad. Dado que los sistemas estadísticos a menudo varían considerablemente de una autoridad competente a otra y que cada autoridad recopila los datos de diferentes fuentes, con diferentes métodos y los gestiona con diferentes criterios y/o utilizando diferentes bases de datos sin interoperabilidad entre estas, la ciberdelincuencia no puede ser objeto de seguimiento con un único sistema estadístico.

- En muchos Estados miembros, los datos sobre ciberdelincuencia consignados en los sistemas estadísticos respectivos son muy escasos. En estas circunstancias, pueden surgir dudas sobre la eficacia de la detección, el procesamiento y el castigo de la ciberdelincuencia y sobre la exactitud de los datos estadísticos.

RECOMENDACIONES

- ***Se exhorta a los Estados miembros que se enfrentan a problemas relativos a la falta de definición común o de interpretación común de la ciberdelincuencia a que elaboren una definición (o interpretación) nacional coherente de la ciberdelincuencia que apliquen todas las partes afectadas en la lucha contra la ciberdelincuencia y con objeto de recabar estadísticas.***

- ***Se exhorta asimismo a los Estados miembros a que recaben estadísticas específicas e independientes sobre la ciberdelincuencia en sentido estricto, la delincuencia favorecida por el ámbito cibernético y los incidentes de seguridad cibernética, que permitan tanto comprobar las cifras globales de ciberdelincuencia como determinar la proporción que representa la ciberdelincuencia dentro de la delincuencia en general.***

- ***Se exhorta a los Estados miembros a que elaboren un modelo normalizado de recopilación de estadísticas generales en todas las diferentes etapas de los procesos penales, desglosadas por ámbitos específicos de ciberdelincuencia, preferentemente los definidos por la UE, esto es, el abuso sexual de menores en línea, el fraude en línea con tarjetas de pago y los ciberataques.***

- ***Los Estados miembros deben estudiar soluciones que permitan la interoperabilidad de las diversas bases de datos que contienen cifras sobre ciberdelincuencia, con el fin de resolver rápidamente la identificación de los delincuentes, la cualificación de los casos y su comparación.***

- ***Los Estados miembros deben facilitar el intercambio de datos estadísticos entre las distintas autoridades nacionales que participan en la lucha contra la ciberdelincuencia, en particular entre los cuerpos y fuerzas de seguridad y las autoridades judiciales.***

VI — ESTRUCTURAS — EL PODER JUDICIAL

CONCLUSIONES Y RECOMENDACIONES CLAVE

- La estructura y la organización del poder judicial varían según los distintos Estados miembros, y con ella la atribución de competencias para entender de los casos de ciberdelincuencia.

- Debido al rápido desarrollo de las TIC y a la complejidad y la sofisticación cada vez mayor de la ciberdelincuencia, el éxito de las investigaciones, los procesamientos y las condenas en los casos de ciberdelincuencia depende, en gran medida, de la habilidad y la experiencia de las autoridades encargadas de la investigación y del juicio. Por ello es de la máxima importancia un buen nivel de comprensión y conocimiento, así como de especialización de la judicatura en este ámbito.

- No obstante, según las conclusiones de la evaluación recíproca, el grado de especialización y de conocimientos específicos de los fiscales y jueces que se ocupan de asuntos relacionados con la ciberdelincuencia y delitos conexos no siempre es satisfactorio.

- En un número importante de Estados miembros, de la ciberdelincuencia se ocupan las Fiscalías generales, y no en todos los Estados miembros existen tribunales especializados o jueces nombrados para examinar y juzgar los delitos informáticos. Sin embargo, algunos Estados miembros sí cuentan con fiscales especializados o estructuras especializadas en las fiscalías que se ocupan de los actos de ciberdelincuencia. En algunos Estados miembros la responsabilidad de tratar esos delitos suele recaer, de hecho, en fiscales y jueces especializados, que han recibido formación o poseen experiencia en el ámbito de la ciberdelincuencia.

- En algunos Estados miembros, existen redes nacionales de ciberfiscales especializados en ciberdelincuencia, lo que puede considerarse una buena práctica, puesto que permite el intercambio de conocimientos y experiencia, y facilitar la difusión de las buenas prácticas entre los profesionales.

- Los evaluadores han recomendado a los Estados miembros que faciliten, con la ayuda de Eurojust, la creación de una red europea de jueces especializados en la lucha contra la ciberdelincuencia, con el fin de mejorar y facilitar la cooperación judicial en este ámbito. Entre tanto, este objetivo se ha conseguido con la creación, en junio de 2016, mediante unas Conclusiones del Consejo, de la Red judicial europea sobre ciberdelincuencia, que ya ha empezado a funcionar.
  Los conocimientos y la experiencia que se intercambien a través de esta red podrán contribuir a una mayor especialización de la judicatura de los Estados miembros.

RECOMENDACIONES
• ***Los Estados miembros deben aumentar el nivel de especialización de su sistema judicial, con el fin de procesar y sancionar eficazmente la ciberdelincuencia en sentido estricto y la delincuencia favorecida por el ámbito cibernético. Para ello, deben considerar la creación de salas o estructuras/unidades internas especializadas o nombrar a fiscales y jueces especializados con un buen nivel de comprensión y conocimiento de la ciberdelincuencia, para encargarse de estos casos.***
• ***Los Estados miembros deben considerar el establecimiento de redes de jueces y fiscales especializados en ciberdelincuencia en el ámbito nacional, como otro instrumento más para hacer más eficaz la lucha contra este tipo de delito.***

VII — ESTRUCTURAS — LOS CUERPOS Y FUERZAS DE SEGURIDAD

CONCLUSIONES Y RECOMENDACIONES CLAVE

- La estructura y la organización de los cuerpos y fuerzas de seguridad varían significativamente de un Estado miembro a otro, en particular en lo que respecta a la atribución de las competencias en relación con la ciberdelincuencia. En algunos Estados miembros, existen unas unidades especializadas que operan con un planteamiento dual, en el que intervienen actividades de planificación estratégica y operativas, mientras que en otros Estados miembros, estas funciones las realizan por separado distintas autoridades y organismos.

- Para hacer frente con eficacia a este tipo de delincuencia son elementos clave la organización eficaz, la integración internacional y la competencia profesional de cuerpos y fuerzas de seguridad que intervienen en la investigación del delito informático. También es esencial para combatir eficazmente esta forma de delincuencia compleja y sofisticada, un buen nivel de conocimientos y de especialización de los cuerpos y fuerzas de seguridad, por los mismos motivos que indicábamos en relación con el poder judicial.

- En términos generales, la evaluación recíproca mostró que el grado de especialización es superior en los cuerpos y fuerzas de seguridad que en el poder judicial, pero que en muchos casos puede mejorarse.

- En la mayoría de los Estados miembros existen en el Ministerio del Interior o en la Policía estructuras o unidades centrales especializadas en ciberdelincuencia, que se encargan de impedir y combatir la ciberdelincuencia a nivel nacional, garantizando así la coordinación de la investigación de la ciberdelincuencia en todo el país con un alto nivel de especialización en este ámbito. Esto facilita también la comunicación entre la Policía y los fiscales. En varios Estados miembros existen también, en los ámbitos local y regional, unidades especializadas descentralizadas que se ocupan específicamente de las investigaciones en materia de ciberdelincuencia.

- Se ha recomendado a algunos Estados miembros que continúen con la reorganización de la Policía y tomen las correspondientes medidas en relación con el aumento de los recursos humanos, la oferta a la policía de una formación más eficaz e intensiva y la dotación de equipo técnico suficiente dedicado a la lucha contra la ciberdelincuencia. Asimismo, es preciso actualizar constantemente los equipos y recursos de los cuerpos y fuerzas de seguridad para hacer frente al desarrollo y diversificación constantes del *modus operandi* de la ciberdelincuencia.

- Los principales obstáculos al éxito de la investigación de la ciberdelincuencia son, entre otros, el rápido desarrollo de la tecnología y la complejidad actual de su *modus operandi*, la profesionalidad y el grado de pericia cada vez mayores de los ciberdelincuentes, el hecho de que la ciberdelincuencia puede abarcar fácilmente la jurisdicción de varios países, la dificultad de obtener pruebas electrónicas en relación con la ciberdelincuencia y los retos relacionados con el recurso al cifrado, a Tor y a la anonimización.

RECOMENDACIONES

- ***Los Estados miembros deben mantener y, en su caso, aumentar el nivel de especialización de los cuerpos y fuerzas de seguridad que se ocupan de las investigaciones en materia de ciberdelincuencia. Los Estados miembros que aún no lo hayan hecho deben considerar la creación de unidades especializadas dentro de los cuerpos y fuerzas de seguridad para luchar contra la ciberdelincuencia con más eficacia, también en los ámbitos regional y local.***

- ***Los Estados miembros deben considerar la creación de una red de policías especializados en la lucha contra la ciberdelincuencia a nivel nacional que pueda contribuir también a mantener un canal de comunicación de los sectores público y privado a la policía.***

- ***Los Estados miembros deben considerar el refuerzo del personal no técnico de la policía en las estructuras locales o regionales y de dotarle de equipo técnico suficiente para cubrir sus necesidades.***

VIII — COOPERACIÓN Y COORDINACIÓN A NIVEL NACIONAL

CONCLUSIONES Y RECOMENDACIONES CLAVE

- Dado que la ciberdelincuencia tiene un carácter transversal y que la responsabilidad de la seguridad del ciberespacio en el ámbito nacional suele estar repartida entre varias entidades con diferentes competencias y capacidades, ya sean públicas o privadas, militares o civiles, colectivas o individuales, un planteamiento pluridisciplinario es clave para prevenir y combatir eficazmente la ciberdelincuencia y garantizar la ciberresiliencia.

- En este contexto, son esenciales una coordinación y cooperación interinstitucionales estrechas y eficaces entre las diferentes autoridades y organismos públicos en los ámbitos operativo y estratégico, así como entre la administración central y las administraciones locales y regionales, con el fin de coordinar las iniciativas y reforzar el intercambio de datos, el apoyo técnico y las técnicas de investigación.

- La cooperación en la lucha contra la ciberdelincuencia entre la Policía, el Ministerio Público y los servicios nacionales de inteligencia puede ser útil también, en la medida en que lo permite la separación estricta de funciones y autoridades entre estas instituciones, tal como exigen algunos Estados miembros, para recibir apoyo desde el punto de vista técnico (interceptaciones, conocimientos, etc.) o información para las investigaciones y procedimientos penales, en particular para la obtención y el tratamiento de pruebas digitales.

- La cooperación entre los sectores público y privado también es crucial para el éxito de la investigación, procesamiento y condena de la ciberdelincuencia en sentido estricto y de la delincuencia favorecida por el ámbito cibernético, así como para la respuesta a las amenazas y ataques cibernéticos (para más detalles, véase el capítulo siguiente).

- Junto con el marco jurídico para la cooperación entre las agencias, cuando este está definido, suelen ser la estrategia nacional de ciberseguridad y el plan de acción para su aplicación (cuando existe) los que definen el marco general de coordinación y cooperación entre todas las instituciones y autoridades públicas con responsabilidades en el ámbito de la ciberseguridad, así como con el sector privado, a fin de garantizar la delimitación de las funciones y responsabilidades.

- La aplicación correcta de la estrategia nacional de ciberseguridad es, por tanto, un factor clave para facilitar las sinergias y maximizar la preparación, así como la capacidad de reacción, en la lucha contra la ciberdelincuencia y el refuerzo de la ciberseguridad.

- Según las conclusiones de las evaluaciones, las formas, modalidades y niveles de cooperación y coordinación entre las partes interesadas implicadas en la lucha contra la ciberdelincuencia y en garantizar la ciberseguridad varían de un Estado miembro a otro. En algunos Estados miembros no existe marco jurídico para la cooperación entre los organismos competentes en los asuntos relativos a la ciberdelincuencia y las autoridades que participan en la lucha contra la ciberdelincuencia cooperan de manera informal. Algunos Estados miembros han instaurado formas de interacción más avanzadas y eficaces, que en los distintos informes han sido definidas como buenas prácticas.

- La mejor manera de garantizar el correcto funcionamiento del sistema es un mecanismo estructurado, especialmente cuando las funciones de coordinación para las cuestiones de ciberseguridad y para las políticas contra la ciberdelincuencia están atribuidas a una autoridad institucional única (es decir, los ministerios o direcciones de su estructura organizativa) o a un organismo o entidad único «ad hoc». Dicha institución u organismo único, que proporciona un marco institucional para la cooperación en el que están representadas las partes interesadas públicas y privadas que participan en la lucha contra la ciberdelincuencia y velan por la ciberseguridad, existe ya en algunos Estados miembros, y en el momento de la evaluación, otros Estados miembros estaban estudiando su creación.

- Algunos Estados miembros en los que se han detectado carencias en el contexto de la evaluación recíproca están haciendo esfuerzos para reforzar las estructuras y procesos de cooperación y coordinación existentes, con el fin de prevenir y combatir más eficazmente la ciberdelincuencia.

RECOMENDACIONES

- ***Los Estados miembros deben dar prioridad a la coordinación y cooperación institucionales entre todas las partes interesadas que participan en la lucha contra la ciberdelincuencia y velan por la ciberseguridad, conforme a un planteamiento pluridisciplinario, con vistas a crear sinergias y a maximizar la preparación y la capacidad de reacción.***

- ***Para ello, se exhorta a los Estados miembros, en particular, a instaurar o reforzar un marco estructurado de colaboración y, si es posible, crear un organismo, entidad o plataforma central en el que estén representados los sectores público y privado, con funciones de coordinación y poder para recomendar soluciones a los problemas detectados.***

IX — LA COOPERACIÓN ENTRE LOS SECTORES PÚBLICO Y PRIVADO

CONCLUSIONES Y RECOMENDACIONES CLAVE

- Una estrecha cooperación entre el sector público y el sector privado es de vital importancia, ya que la lucha contra la ciberdelincuencia es muy compleja, lo que significa que los cuerpos y fuerzas de seguridad no consiguen combatir este delito sin la cooperación del sector privado (entidades financieras o bancarias, compañías de telecomunicaciones, proveedores de servicios de Internet, ONG, universidades, empresas, asociaciones profesionales, etc.).

- Dicha cooperación podría obrar en beneficio de ambos sectores, pues brinda la oportunidad de implicar a una amplia gama de entidades que colaboran y de crear sinergias entre ellas, contribuyendo así a aumentar el nivel de ciberseguridad.

- La contribución de las partes interesadas del sector privado en cuanto a conocimientos, asistencia técnica e intercambio de información sobre las amenazas cibernéticas y la ciberseguridad es de gran valor añadido para el éxito de las investigaciones y de las acciones emprendidas para resolver los ciberincidentes. También es útil implicar a los fiscales en los contactos con el sector privado, con objeto de garantizar que las pruebas se reúnan en cumplimiento de la legislación vigente y sean admisibles en los procedimientos judiciales.

- Según los resultados de la evaluación, el nivel de cooperación entre el sector público y el privado varía de un Estado miembro a otro y, por lo general, demuestra ser más desarrollado y eficiente cuando es más estructurado y cuando existe un entorno de confianza y seguridad. En algunos Estados miembros, la evaluación ha detectado buenas prácticas, mientras que en otros se ha puesto de relieve la necesidad de mejorar dicha cooperación.

- En las estrategias de ciberseguridad nacionales de algunos Estados miembros está previsto el recurso a asociaciones público-privadas, pero a veces se limita a ámbitos específicos. Puede basarse en memorandos de acuerdo o en acuerdos informales similares.

- Sin embargo, no todos los Estados miembros han desarrollado un marco formal para las asociaciones público-privadas, y en algunos de ellos la cooperación, las reuniones y los intercambios de información con el sector privado sobre los incidentes, las tendencias y las novedades tienen lugar de manera informal, sin base jurídica.

- Las formas más avanzadas de cooperación con el sector privado se han observado en algunos Estados miembros donde esta cooperación se ha institucionalizado mediante la creación de instituciones o grupos de trabajo apropiados con vistas a la cooperación entre el sector privado y la administración pública y los organismos policiales.

- Según las conclusiones de la evaluación, los evaluadores consideran que las asociaciones público-privadas son un importante instrumento para la correcta cooperación entre los cuerpos y fuerzas de seguridad y el sector privado, y sobre todo con los proveedores de servicios de Internet y con el sector financiero, en particular los bancos, pero también con las ONG, los CSIRT y los operadores de las infraestructuras críticas. Pueden resultar útiles para eliminar contenidos ilícitos, así como para el descifrado y la respuesta a ciberataques.

- La cooperación con los proveedores de servicios es especialmente útil, tanto para aprovechar su experiencia como para acceder a la información básica sobre los abonados. Mediante la realización de análisis de riesgos, la toma de las medidas de seguridad oportunas y la aplicación de una política de seguridad estructurada, los proveedores de redes y servicios de comunicaciones electrónicas pueden no solo impedir la aparición de ciertos tipos de ciberdelincuencia, sino también asistir a los cuerpos y fuerzas de seguridad al facilitar pruebas.

- Según las conclusiones de la evaluación, es necesario definir soluciones para un marco claro y apropiado que regule las relaciones de las autoridades judiciales con los proveedores de servicios de Internet en toda la UE. Para ello, disponer de unos procedimientos que puedan permitir a las autoridades recibir puntualmente respuestas a sus solicitudes, y poner en práctica un sistema de sanciones en caso de incumplimiento, denegación de cooperación y omisión (multas administrativas o procesales) podría mejorar esta cooperación.

- Un diálogo con los principales operadores de Internet, empresas de alojamiento de datos y proveedores de acceso a Internet o servicios, tanto de la UE como de ámbito internacional, podría reforzar su cooperación en el marco de las investigaciones penales.

- Una cooperación eficaz entre las fuerzas y cuerpos de seguridad, por una parte, y las entidades financieras y los bancos comerciales, por otra, es también esencial en la lucha contra el fraude con tarjeta no presente y otros tipos de fraude en línea, con el fin de detectar estos fraudes, poner al corriente al sector privado de nuevas tendencias y definir medidas cautelares.

- En algunos Estados miembros, esta cooperación se ve facilitada por asociaciones de banca o comités interbancarios creados exclusivamente para luchar contra el fraude en los sistemas y medios de pago, que se reúnen periódicamente, con la participación de la Policía. En un Estado miembro, los evaluadores consideraron que la participación de la Policía en el órgano consultivo de la asociación nacional de banca constituía una buena práctica.

- En otros Estados miembros, la cooperación entre las fuerzas y cuerpos de seguridad y las instituciones bancarias y financieras está menos estructurada y se limita a contactos o reuniones para garantizar la colaboración y el intercambio de información sobre cuestiones relacionadas con la ciberdelincuencia.

- En algunos Estados miembros existe para el sector privado una obligación de información sobre ciberdelincuencia; en otros Estados miembros, en cambio, esta obligación de notificación no existe, o bien se circunscribe a determinadas ramas del sector privado o a determinados tipos de ciberdelitos.

- En algunos casos, la información sobre la ciberdelincuencia se efectúa con carácter voluntario. No obstante, según las conclusiones de las evaluaciones, en algunos Estados miembros, las entidades financieras y de crédito y los proveedores de servicios de Internet son reacios a informar y a apoyar un procedimiento penal con el objetivo de determinar la responsabilidad penal del autor. Les interesa más limitar lo antes posible los daños que pudieran derivarse de una publicación y un interés de los medios de comunicación que no convienen a su credibilidad y reputación.

- Según determinados informes, cuando el sector privado es la víctima o la parte perjudicada, la cooperación con las fuerzas y cuerpos de seguridad suele ser buena, puesto que se encarga de la conservación de las pruebas, su interpretación y su entrega a las citadas fuerzas.

- El sector privado desempeña también un papel importante en la protección de los menores y en actividades de prevención y concienciación a este respecto; las asociaciones privadas y las ONG que operan en este ámbito cooperan con las fuerzas y cuerpos de seguridad que participan en la lucha contra la explotación sexual en línea y aportan una contribución clave al canalizar las denuncias de abusos.

- Según las conclusiones de la evaluación, un diálogo con el sector privado más allá de los requisitos de información obligatorios facilitaría, de todos modos, la consecución de mejores resultados en la lucha contra los delitos informáticos.

- Las autoridades públicas deberían cooperar también, como ocurre en varios Estados miembros, con las universidades, las instituciones educativas, los servicios sociales, las empresas, las asociaciones profesionales, los medios de comunicación y otras organizaciones y empresas a fin de impedir y neutralizar el impacto negativo de la delincuencia informática en sentido estricto y la delincuencia favorecida por la informática en la seguridad de la información en el país. En particular, la cooperación con la universidad es muy importante para la sensibilización, la formación y la investigación y el desarrollo (I+D).

RECOMENDACIONES

- ***Los Estados miembros y las instituciones de la UE deben seguir reflexionando sobre la manera de mantener y aumentar la cooperación entre el sector público y el privado (bancos, empresas de telecomunicaciones y proveedores de servicios), lo que incluye la participación de los fiscales y, en su caso, de los jueces.***

- ***Los Estados miembros deben recurrir a las asociaciones público-privadas estructuradas, con el fin de disponer un marco claro para la cooperación entre el sector público y el privado con normas y funciones claras, distinguiendo quizás entre medidas preventivas, por una parte, e investigación y procesamiento, por otra.***

- ***Los Estados miembros deben alentar al sector privado a compartir información con las autoridades públicas y, en su caso, prever en la legislación nacional la obligación para el sector privado de informar sobre incidentes de seguridad informática, en particular la obligación a las entidades de crédito y otras infraestructuras críticas de comunicar inmediatamente incidencias relativas al ámbito cibernético que afecten tanto a las entidades de crédito como a sus clientes.***

- ***La Unión Europea y sus Estados miembros deben seguir reflexionando sobre la manera de mejorar la cooperación entre los cuerpos y fuerzas de seguridad de los Estados miembros y los proveedores de servicios, lo que incluye la posibilidad de que la UE celebre acuerdos con algunos de ellos a fin de reforzar la cooperación en el marco de las investigaciones judiciales.***

X — TÉCNICAS DE INVESTIGACIÓN

CONCLUSIONES Y RECOMENDACIONES CLAVE

- La gran variedad de los ciberdelitos impide que existan procesos o métodos generalmente probados y ensayados para investigar dichas infracciones. Cada investigación y cada planteamiento depende de sus circunstancias particulares, por lo que los procedimientos y métodos de investigación deben adaptarse a cada caso concreto.

- Sobre todo en el ámbito de la ciberdelincuencia, el *modus operandi*, los programas informáticos y las herramientas que se utilizan cambian constantemente y a intervalos cortos. Las técnicas de investigación deben por tanto actualizarse constantemente (por ejemplo, con programas informáticos especiales de investigación), en consonancia con la evolución de la ciberdelincuencia.

- Para la investigación de los delitos informáticos se utilizan técnicas especiales además de las técnicas de investigación ordinarias. Hay varias posibilidades: las técnicas de investigación especiales de uso más común, que son herramientas de trabajo particularmente eficaces en particular cuando se aplican a casos en los que interviene explotación sexual de menores, son la interceptación de las comunicaciones, la conservación de los datos y la investigación encubierta.
  Esta última, especialmente útil si la investigación no puede llevarse a cabo utilizando medios técnicos, se realiza mediante agentes encubiertos para llevar a cabo investigaciones en los foros y tablones. Sin embargo, las investigaciones de este tipo solo tienen probabilidades de rendir resultados satisfactorios si se prolongan en el tiempo.

- Otras técnicas especiales de investigación se basan en las nuevas posibilidades técnicas de la lucha contra la delincuencia informática en línea, como la observación en línea u otras técnicas tales como el bloqueo del acceso al soporte físico («hardware») y las copiadoras de bits especiales, el registro e incautación a distancia (por ejemplo el caso en que los cuerpos y fuerzas de seguridad intervienen en línea un ordenador sospechoso en lugar de tomarlo físicamente), el seguimiento de IPs, las búsquedas de fuente abierta en Internet, la copia de seguridad de datos procedentes de soportes de datos y de Internet (sitios web, registros). También se utilizan técnicas especiales para los dispositivos móviles (por ejemplo, los UFED).

- Sin embargo, la legislación nacional de los Estados miembros no siempre prevé el recurso a técnicas especiales de investigación. En algunos Estados miembros es necesaria una orden judicial para este fin.

RECOMENDACIONES
• ***Se exhorta a los Estados miembros que aún no lo hayan hecho a que establezcan en su Derecho nacional la posibilidad de recurrir a técnicas especiales de investigación, con el fin de facilitar las investigaciones en los casos de ciberdelincuencia.***

XI - CIFRADO

CONCLUSIONES Y RECOMENDACIONES CLAVE

- La creciente disponibilidad y uso de tecnologías de cifrado seguras y fiables garantiza la seguridad, la protección de la transmisión y la confidencialidad de los datos informáticos y, por consiguiente, la protección de la intimidad de los ciudadanos y la protección efectiva de los datos en el ciberespacio.

- Sin embargo, el recurso cada vez más frecuente al cifrado, tanto en el almacenamiento de datos como en las comunicaciones por Internet, unido a la sofisticación cada vez mayor de las técnicas, hace cada vez más difícil, si no prácticamente imposible, el pasar a través del cifrado, lo cual está llegando a ser un problema en todos los Estados miembros.

- A menudo son los propios delincuentes los que recurren al cifrado para proteger el material ilícito que está en su poder y sus comunicaciones, lo que dificulta la investigación de la ciberdelincuencia. Dado que muchas aplicaciones utilizan el cifrado por defecto, las fuerzas y cuerpos de seguridad a menudo tienen dificultades en la obtención de pruebas que están en forma cifrada.

- El cifrado dificulta o impide totalmente el acceso a información pertinente en relación con la ciberdelincuencia, en particular para la identificación de las comunicaciones o de los datos informáticos en posesión de los sospechosos o los infractores, no solo en los exámenes periciales sino también en los demás tipos de investigaciones. Además, el recurso al cifrado de extremo a extremo por un número cada vez mayor de proveedores de servicios dificulta la interceptación o la interpretación del material.

- No existe solución normalizada ni para los datos cifrados ni para las comunicaciones cifradas. Tras el examen del caso concreto, puede recurrirse a medidas selectivas, tales como medidas extraordinarias de vigilancia de las telecomunicaciones o medidas de descifrado.

- En este contexto, la primera dificultad es detectar el contenido cifrado y la forma de cifrado utilizando el equipo necesario. El problema más importante es, sin embargo, el propio descifrado, que solo es posible recurriendo a material y programas informáticos especializados de gran capacidad que suponen elevadas inversiones y costes significativos.

- Para hacer frente a estos problemas es necesario conocer con profundidad la tecnología de cifrado más reciente y estudiar los puntos débiles de los algoritmos y aplicaciones, incluso para aprovechar los posibles errores.

- La evaluación ha puesto de manifiesto que con frecuencia se logra algún éxito cuando se emplean formas muy sencillas de métodos de cifrado, y que es posible averiguar o calcular retrospectivamente las claves utilizando el programa informático adecuado que posibilita el descifrado. Las contraseñas sencillas pueden descifrarse utilizando el material informático y las herramientas adecuados.

- Las autoridades investigadoras pueden contribuir de manera significativa al éxito del descifrado de contraseña si son capaces de facilitar a los peritos en informática forense información relativa a la contraseña misma (posibles frases, fragmentos de frase, conjuntos de caracteres, longitud de la contraseña, etc.), y todas las pruebas electrónicas o los dispositivos. Ahora bien, esto no siempre es eficaz.

- Según las conclusiones de la evaluación, en algunos casos se han descifrado con éxito cifrados más complejos lanzando ataques de fuerza bruta (es decir ataques en los que se introducen todos los códigos posibles) o de diccionario (es decir empleando términos específicos para la extracción de contraseñas), o cuando el sospechoso ha aceptado cooperar y ha proporcionado la contraseña o frase necesaria para el descifrado. Sin embargo, los interesados no siempre están dispuestos a cooperar con las autoridades y no existen medios para obligarlos a hacerlo.

- Cuando los archivos están protegidos con un alto nivel de cifrado (por ejemplo, archivos cifrados mediante el algoritmo AES-256) o en casos de discos completamente cifrados (por ejemplo, mediante TrueCrypt, BitLocker, FileVault2, WinRar o PGP), emplear ataques de fuerza bruta o de diccionario puede llevar mucho tiempo (meses, incluso años, en algunos casos) y requiere una gran capacidad de computación (programas informáticos comerciales especializados e infraestructura de clúster en red). Puede ocurrir que, pese a todo, sea imposible romper la protección criptográfica si los autores usan contraseñas técnicamente avanzadas o algoritmos complejos, y en determinados casos se abandona el proceso de descifrado.

- En algunos Estados miembros, el descifrado se lleva a cabo en cooperación con empresas privadas cuyo conocimiento experto resulta especialmente útil en los casos en los que los métodos de cifrado son muy sofisticados. Por el contrario, en numerosos Estados miembros las empresas privadas no están involucradas en el descifrado en el marco de las investigaciones penales, coto reservado a los Institutos Nacionales de Criminalística.

- Los recursos y servicios de Europol, en particular su Centro Europeo de Ciberdelincuencia (EC3), ofrecen una plataforma de descifrado de la que pueden hacer uso algunos Estados miembros.

- Según las conclusiones de la evaluación, se pueden resolver en parte las dificultades que plantea el cifrado mediante un refuerzo de la investigación y la elaboración de nuevos métodos, por ejemplo un análisis más inteligente del patrón o patrones de creación de contraseñas del sospechoso o la agregación dinámica de la capacidad de computación.

- Una buena cooperación entre las distintas autoridades implicadas, en particular entre las fuerzas y cuerpos de seguridad, los expertos en informática forense y la fiscalía, es también indispensable, especialmente porque, a causa de su precio, no todos los departamentos o autoridades pueden permitirse la compra de programas y material informáticos para la recuperación de contraseñas.

- El intercambio de recursos y experiencias y la participación en operaciones conjuntas garantizan la cooperación entre los Estados miembros en el ámbito del descifrado. Los canales de Europol o Interpol permiten, en caso de necesidad, remitir pruebas a otras autoridades para su descifrado.

RECOMENDACIONES

- ***Los Estados miembros deben invertir en material y programas informáticos especializados con una capacidad de computación adecuada y en personal con una formación adecuada a fin de garantizar el descifrado también en casos complejos de archivos y comunicaciones cifrados.***

- ***Los Estados miembros deben garantizar la cooperación entre todas las partes interesadas pertinentes, incluyendo, si procede, a las empresas privadas, a fin de aumentar las capacidades de descifrado de las autoridades competentes.***

- ***Los Estados miembros deben reforzar la investigación y el desarrollo con el objetivo de desarrollar nuevos métodos más eficientes de descifrado así como utilizar los recursos de Europol, a saber, la plataforma de descifrado del Centro Europeo de Ciberdelincuencia (EC3) para los casos más sofisticados de cifrado.***

- ***Se recomienda a los Estados miembros y a las instituciones de la UE que consideren soluciones e intensifiquen un diálogo abierto con el sector privado.***

XII - PRUEBAS ELECTRÓNICAS

CONCLUSIONES Y RECOMENDACIONES CLAVE

- La legislación nacional de un importante número de Estados miembros carece de una definición de «prueba electrónica». Los términos empleados en el Convenio sobre la Ciberdelincuencia del Consejo de Europa (en lo sucesivo, «el Convenio de Budapest») y en la Directiva 2013/40/UE, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información, sirven de referencia.

- En la práctica, por lo general se entiende por «prueba electrónica» cualquier información generada, almacenada o transmitida mediante equipos electrónicos y susceptible de demostrar la existencia o la no existencia de un delito, de identificar a la persona que cometió dicho delito y de determinar las circunstancias necesarias para la resolución de un caso.

- Así pues, puede tratarse de: información de registro, historiales de navegación, contenido de datos, imágenes, direcciones IP, correos electrónicos, documentos electrónicos, archivos de vídeo digitales, archivos de sonido e imágenes, bases de datos, hojas de datos, cookies, documentos electrónicos impresos, contabilidad electrónica, datos de geolocalización por GPS, registros de las operaciones bancarias realizadas, etc.

- La recopilación, el análisis y el uso de pruebas electrónicas son cada vez más pertinentes en el marco de los procesos penales, no solo relativos a ciberdelitos sino también a cualquier otro delito que pueda incluir pruebas electrónicas.

- La naturaleza de las pruebas electrónicas y la facilidad con la que pueden ser manipuladas o falsificadas pueden crear problemas en lo que respecta a su admisibilidad, que no se dan con otros tipos de pruebas.

  Por esta razón, en algunos Estados miembros existen requisitos específicos en lo que respecta a la recopilación de pruebas electrónicas para que sean admisibles en los tribunales. Por ejemplo, pueden consistir en que la recopilación sea realizada por un experto con conocimiento técnico a fin de preservar la integridad de las pruebas electrónicas o en que se documente adecuadamente la cadena de custodia en lo que respecta a cómo se obtuvieron originalmente las pruebas, a quién las ha manejado y cómo y, en particular, a si han sido alteradas de alguna manera.

- Para la recopilación de pruebas electrónicas, algunos Estados miembros siguen las mejores prácticas sobre informática forense establecidas en el Convenio del Consejo de Europea sobre la Ciberdelincuencia o en directrices internacionales como por ejemplo las de la Asociación de Mandos de la Policía (ACPO), que también se aplican al almacenamiento y la transferencia de pruebas electrónicas.

- Sin embargo, la evaluación ha puesto de manifiesto que en la mayoría de los Estados miembros, el Derecho procesal es esencialmente neutro desde el punto de vista tecnológico, lo que significa que se aplican normas y principios generales sobre la obtención de pruebas y que el Derecho procesal no contiene normas específicas sobre la admisibilidad y evaluación de las pruebas electrónicas, que están sujetas a las mismas condiciones que cualquier otro elemento de prueba y son evaluadas por los jueces de conformidad con la Ley de enjuiciamiento penal general.

- En consecuencia, de manera general, las pruebas electrónicas son admisibles en los procesos penales si han sido obtenidas de manera lícita y son pertinentes para el juicio. Ello también se aplica a las pruebas electrónicas recogidas fuera del Estado mediante la cooperación con los Estados miembros en el marco de la asistencia judicial internacional o la cooperación directa con proveedores de servicios de Internet extranjeros.

- Sin embargo, como se indica en uno de los informes particulares, la inexistencia de una reglamentación relativa a la metodología de recopilación y presentación de pruebas electrónicas ante el tribunal no debería, en principio, impedir el procesamiento efectivo de los casos de ciberdelincuencia, puesto que la admisibilidad de las pruebas electrónicas está cubierta por la reglamentación general relativa a las pruebas.

- En algunos Estados miembros, las pruebas electrónicas, como la mayoría de las pruebas tradicionales, son admisibles en los tribunales y evaluadas por el juez de conformidad con los principios de libre apreciación de las pruebas. Ello significa que cualquier cosa que pueda tener valor como prueba en un asunto puede, en principio, ser presentado a un tribunal que decidirá, caso por caso, cuánto valor conceder a cada elemento de prueba. Según las conclusiones de la evaluación, se puede considerar que esto es una buena práctica.

- Cuando, al contrario, las normas sobre la admisibilidad de las pruebas son más bien estrictas, ello puede crear obstáculos para las pruebas electrónicas, especialmente cuando han sido obtenidas en otros países, por ejemplo a través de peticiones de asistencia judicial.

- La policía, provista por lo general de una orden judicial, puede acceder a datos almacenados en el lugar del registro, así como a datos remotos o situados en el extranjero respetando los acuerdos internacionales. Si la clarificación de los hechos pertinentes para los procesos penales requiere, para su introducción en los expedientes penales, la conservación de ciertos datos informáticos almacenados, por ejemplo de datos operativos guardados mediante el sistema informático o almacenados en cualquier soporte de datos (por ejemplo, en CD, DVD o teléfonos móviles), dichos objetos son por lo general incautados de conformidad con las normas de enjuiciamiento penal pertinentes de los Estados miembros.

- Si una prueba electrónica está en Internet, o está en manos de los proveedores de servicios, la cooperación directa con ellos es esencial para obtener los datos necesarios y tomar medidas encaminadas a impedir la pérdida, destrucción o modificación de los datos. Sin embargo, no en todos los Estados miembros se puede acceder directamente a las pruebas electrónicas situadas en otro país o en la nube, y en estos casos se deben seguir los procedimientos de asistencia judicial.

- Según las conclusiones de la evaluación, a fin de abordar dichos problemas, es necesario aumentar la velocidad y la eficiencia de los procedimientos actuales de asistencia judicial, y las autoridades encargadas de la investigación deben tener la posibilidad de enviar muy rápidamente solicitudes a numerosos países distintos.

- En algunos Estados miembros, la legislación nacional permite obtener información directamente de los proveedores extranjeros, siempre que la legislación del Estado en el que se encuentra la sede del proveedor también lo permita. Un marco común para el intercambio de datos de los abonados y nuevos enfoques en el ámbito de la UE sobre la jurisdicción de ejecución son algunos de los asuntos que se están abordando en el trabajo emprendido a escala de la Unión a partir de las Conclusiones del Consejo sobre la mejora de la justicia penal en el ciberespacio, de 9 de junio de 2016.

- Las prácticas para integrar en el expediente del caso, en un formato que permita su estudio por parte de fiscales y jueces, las pruebas electrónicas obtenidas durante la investigación, así como la manera de hacerlo, varían entre los Estados miembros.

- La incautación de material informático que contiene pruebas electrónicas no parece ser la mejor opción, ya que puede resultar difícil para la víctima de un ciberdelito aceptar la pérdida de los equipos digitales que se incautarían durante la investigación.

- Otra posibilidad para hacerse con pruebas electrónicas sería copiar (replicar) los datos almacenados en otro soporte de almacenamiento (por ejemplo, un DVD o un disco duro) y ponerlos a disposición en este formato o, especialmente en el caso de datos legibles (por ejemplo, mensajes de texto) o de archivos de imágenes, imprimirlos y ponerlos a disposición en papel.

- Por lo general, se emplea el mismo procedimiento en el caso de pruebas electrónicas obtenidas en el extranjero. Sin embargo, si el país que ayudó a obtener las pruebas fija condiciones especiales, la policía y la fiscalía tienen que respetarlas.

- Cuando la fiscalía y los jueces que tienen que manejar pruebas electrónicas en procesos judiciales las reciben en un formato que solo permite acceder a ellas y evaluarlas mediante equipos informáticos y, por lo tanto, en particular para analizar su autenticidad, son necesarios conocimientos específicos, se puede pedir consejo a un experto forense.

- Según las conclusiones de la evaluación, material informático y programas específicos de alta tecnología para una mejor identificación y extracción de pruebas electrónicas permitirían a las autoridades de los Estados miembros trabajar y cooperar con pruebas electrónicas comparables.

RECOMENDACIONES

- ***Los Estados miembros deben disponer de material y programas informáticos adecuados de alta tecnología para la identificación y la extracción de pruebas electrónicas que permitan a los Estados miembros trabajar y cooperar con pruebas electrónicas comparables.***

- ***Los Estados miembros deben velar por que su legislación de enjuiciamiento nacional sea suficientemente flexible como para facilitar la admisibilidad de pruebas electrónicas, también en los casos en que se hayan obtenido en otro país, por ejemplo a través de peticiones de asistencia judicial.***

- ***Los Estados miembros deben considerar entablar y mantener, con la posible participación de Eurojust y la Red Judicial Europea sobre Ciberdelincuencia, un diálogo constante con el sector privado y debatir metodologías para garantizar que la recopilación de pruebas electrónicas se realice de una forma que permita su admisibilidad en los tribunales.***

- ***La UE y sus Estados miembros deben estudiar la elaboración de un marco de la UE que establezca las normas de acceso, a efectos del cumplimiento de la ley, a los datos que poseen los proveedores de servicios, de modo que se refleje el resultado de los trabajos en curso de los expertos sobre el acceso a las pruebas electrónicas. Dicho marco debe regular las relaciones entre las fuerzas y cuerpos de seguridad y los proveedores de servicios de Internet, y ha de contener normas y obligaciones claras.***

XIII - COMPUTACIÓN «EN LA NUBE»

CONCLUSIONES Y RECOMENDACIONES CLAVE

- Un importante número de Estados miembros subrayó que los ciberdelitos relacionados con datos almacenados en la nube plantean problemas en lo que respecta a la investigación y el procesamiento.

- Algunos Estados miembros, en el momento de la evaluación, carecían de experiencia en investigaciones de ciberdelitos de este tipo y, en consecuencia, no se había sometido a examen ante sus tribunales nacionales la cuestión de la jurisdicción en lo relativo al almacenamiento en la nube, lo que en la práctica podría implicar que numerosos casos de ciberdelincuencia no han sido procesados. Sin embargo, se reconoció que, inevitablemente, los Estados tendrán que hacer frente a situaciones de este tipo.

- Este fenómeno puede provocar serios problemas en el futuro ya que las soluciones en la nube son cada vez más populares y el uso de almacenamiento y servicios basados en la nube es una práctica cada vez más común, no solo para personas físicas o jurídicas sino también para delincuentes.

- Las tecnologías empleadas, la capacidad de almacenamiento en los servidores y las economías de escala hacen que los datos se muevan constantemente alrededor del globo y puedan dividirse en piezas que se unen únicamente cuando alguien accede a ellos. Así pues, un problema específico que se plantea a la hora de hacer frente a los delitos relacionados con la nube pues localizar el lugar físico en el que se comete el delito, algo que puede ser difícil, largo y complicado. En consecuencia, las fuerzas y cuerpos de seguridad tienen dificultades para localizar y acceder a la información y a los servidores que alojan datos en la nube.

- La falta de información impide a los investigadores encontrar pistas digitales y puede complicar la identificación del autor, del momento del delito, de su situación geográfica y del instrumento empleado para cometerlo, y ello da lugar a casos en los que un ciberdelito puede quedar impune y a situaciones en las que algunas personas serán víctimas una y otra vez.

- Por otra parte, los proveedores de almacenamiento en la nube pueden tener dificultades para situar la verdadera ubicación (espacial) de los datos; incluso los propietarios de los datos ignoran a menudo dónde se encuentran estos.

- Puesto que los delitos relacionados con datos almacenados en la nube pueden situarse dentro de la jurisdicción de varios Estados miembros o también fuera de la UE, la computación en la nube plantea problemas no solo en lo que respecta al Derecho nacional, sino también al Derecho internacional, que se basa en la soberanía de los Estados miembros y en el principio de territorialidad.

- Aunque se haya determinado la ubicación, la legislación nacional de algunos Estados miembros no contempla una jurisdicción extraterritorial, o bien estipula que los delitos informáticos relacionados con datos almacenados en la nube solo podrán ser procesados si dichos datos son accesibles desde el Estado miembro en cuestión.

- Pueden surgir conflictos de jurisdicción en lo que respecta a la competencia de emitir una orden para obtener las correspondientes pruebas electrónicas cuando dos o más Estados miembros pueden establecer su jurisdicción sobre el delito; en estos casos, los Estados miembros pueden emplear los servicios de Eurojust y de los equipos conjuntos de investigación para superar dichos conflictos.

- En la evaluación se han observado dos posibilidades principales para obtener datos almacenados en la nube: la primera consiste en obtener un acceso directo al contenido de dichos perfiles y servicios de almacenamiento con el consentimiento del usuario/propietario del perfil o la cuenta. En caso de que sea posible identificar la ubicación de la información, también se puede recurrir a los procedimientos de asistencia judicial, pero ha de tenerse en cuenta que estos suelen ser largos e ineficientes.

- La otra opción, consistente en ordenar directamente a los proveedores que faciliten ciertos datos, resulta a menudo muy difícil de poner en práctica, ya que hay proveedores que no cooperan con las fuerzas y cuerpos de seguridad extranjeros y no responden a todas las solicitudes.

- A fin de superar estas dificultades, la evaluación ha subrayado la posibilidad de llegar a acuerdos especiales con algunos proveedores de servicios en la nube (por ejemplo, Google, Yahoo, etc.) a fin de reducir los plazos y obtener información en formatos admisibles en los tribunales. En el marco de los trabajos en curso de los expertos sobre las pruebas electrónicas, la UE estudia actualmente medidas destinadas a superar este obstáculo, como la creación de ventanillas únicas tanto en los Estados miembros como en los proveedores de servicios, o un marco jurídico de la UE para poder dirigir a los proveedores de servicios medidas de investigación que permitan a las autoridades exhortar («solicitud de presentación») u obligar («orden de presentación») a un proveedor de servicios situado en otro Estado miembro a revelar información sobre un usuario, etc.

- Con arreglo a lo dispuesto en el Convenio del Consejo de Europa sobre la Ciberdelincuencia, la acción transfronteriza solo es posible en un número muy limitado de casos, a saber, cuando se cuenta con el consentimiento legal de la persona que tiene la autoridad legítima para divulgar los datos, en los casos en los que se conoce la jurisdicción. Cuando los datos están situados fuera del territorio de los Estados Partes en el Convenio, dichas disposiciones no son de aplicación.

- A la luz de lo anterior, todavía no ha sido posible solucionar adecuadamente el problema del almacenamiento en la nube. Las diversas posibilidades que ofrece el Derecho internacional para actuar de forma independiente o en el marco de la asistencia judicial han demostrado sus limitaciones en lo que respecta a la investigación de ciberdelitos cuando hay datos almacenados en la nube.

- Según las conclusiones de la evaluación, se debe estudiar cómo mejorar la práctica a fin de garantizar la eficacia de la investigación y el procesamiento de los ciberdelitos relacionados con datos almacenados en la nube, teniendo también en cuenta las dificultades derivadas de los posibles conflictos de jurisdicción.

- Con este fin, podría ser útil estudiar la posibilidad de hacer frente a los problemas ligados a los actuales marcos jurídicos pertinentes y a la investigación, a fin de contar con normas y procedimientos claros en lo que respecta a los ciberdelitos relacionados con datos almacenados en la nube.

- En el contexto de la evaluación, se ha subrayado la utilidad de la participación de los Estados miembros en foros internacionales en los que se debatan soluciones a dichas cuestiones como, por ejemplo, el Comité del Convenio sobre la Ciberdelincuencia.[6]

- Un Estado miembro presentó sugerencias para acceder a datos almacenados en la nube, como imponer a los proveedores de servicios de datos que proporcionen contraseñas a las fuerzas y cuerpos de seguridad para que puedan acceder a los datos u ofrecer la posibilidad de realizar búsquedas virtuales en centros de datos situados en otros países sin tener que determinar en primer lugar la situación geográfica del servidor.

[6] El Comité del Convenio sobre la Ciberdelincuencia ha adoptado el mandato para la negociación de un protocolo adicional que aborde estas cuestiones.

RECOMENDACIONES

- ***Los Estados miembros deben considerar la celebración de acuerdos especiales con los principales proveedores de servicios en la nube a fin de reducir los plazos y obtener datos admisibles en los tribunales.***

- ***La UE debe seguir abordando los retos mundiales que plantea la computación en nube con el fin de identificar soluciones que podrían aumentar la capacidad de investigar la ciberdelincuencia, también en el contexto los trabajos en curso de los expertos sobre las pruebas electrónicas.***

XIV - CONSERVACIÓN DE LOS DATOS PROCEDENTES DE COMUNICACIONES ELECTRÓNICAS

CONCLUSIONES Y RECOMENDACIONES CLAVE

- La anulación de la Directiva 2006/24/CE, debido a la sentencia del Tribunal de Justicia de 8 de abril de 2014 (asuntos acumulados C-293/12 y C-594/12, «Digital Rights Ireland y Seitlinger y otros»), ha creado una situación de inseguridad jurídica, en particular por lo que respecta al estatuto jurídico de la legislación nacional de transposición. Los Estados miembros están reaccionando de manera diferente a la sentencia, ya sea mediante el mantenimiento, la modificación, la sustitución o la derogación de la legislación de transposición, o su anulación por los tribunales nacionales.

- Varios Estados miembros han subrayado las consecuencias negativas de la sentencia anteriormente mencionada en lo que respecta a la eficacia de las investigaciones y procesamientos penales en el ámbito nacional, en particular en lo que se refiere a la fiabilidad y admisibilidad ante los tribunales de pruebas basadas en la recopilación de datos de comunicaciones electrónicas, así como a la cooperación judicial transfronteriza, tanto entre los Estados miembros como a escala internacional (capacidad limitada para proporcionar y obtener pruebas). La falta de conservación de datos o su conservación solo durante un período limitado dificulta o incluso imposibilita la obtención de pruebas electrónicas en los Estados miembros de la UE.

- Varios Estados miembros han hecho hincapié en que un enfoque común a escala de la UE aportaría valor añadido, lo que incluye la posibilidad de crear un nuevo marco legislativo que podría armonizar las condiciones y los períodos de conservación de datos en los Estados miembros.

- Entretanto, en su sentencia sobre los dos asuntos acumulados C-203/15 y C-698/15 de 21 de diciembre de 2016, «Tele2 y Watson», el Tribunal de Justicia afirmó que toda legislación nacional que imponga la conservación generalizada de todos los datos de tráfico y de localización supera los límites necesarios y clarificó los criterios y condiciones que deben cumplir los regímenes nacionales de conservación de datos de los Estados miembros.

- Actualmente se está llevando a cabo un proceso de reflexión común entre las instituciones de la UE y los Estados miembros para abordar la cuestión de la conservación de los datos con el fin de identificar soluciones jurídicas y prácticas a los retos conexos derivados de la jurisprudencia del Tribunal de Justicia.

RECOMENDACIONES
• ***Los Estados miembros y las instituciones de la UE deben continuar la reflexión común con vistas a encontrar soluciones jurídicas y prácticas para abordar la cuestión de la conservación de los datos procedentes de comunicaciones electrónicas a escala nacional y de la UE, teniendo en cuenta los principios consagrados en la reciente jurisprudencia del Tribunal de Justicia.***

XV - ACCIONES CONTRA LA PORNOGRAFÍA INFANTIL Y EL ABUSO SEXUAL DE MENORES EN LÍNEA

CONCLUSIONES Y RECOMENDACIONES CLAVE

- En el momento de la evaluación, la mayoría de los Estados miembros había transpuesto la Directiva 2011/93/UE del Parlamento Europeo y del Consejo, de 13 de diciembre de 2011, relativa a la lucha contra los abusos sexuales y la explotación sexual de los menores y la pornografía infantil. El estado actual de la incorporación de dicha Directiva en las diferentes legislaciones nacionales se puede consultar en: http://eur-lex.europa.eu/legal-content/EN/NIM/?uri=celex:32011L0093

- Las evoluciones sociales y los avances tecnológicos han aumentado tanto las oportunidades de comunicación y de difusión de la información como las posibilidades de cometer delitos en línea, por lo que el abuso sexual de menores en Internet (captación de menores, sexteo, ciberacoso, etc.) se ha agravado considerablemente en los últimos años. A fin de luchar de manera eficaz contra dichas formas de delincuencia, se está aplicando en los Estados miembros un amplio abanico de medidas preventivas y coercitivas, en las que participan el sector público y el privado.

- En algunos Estados miembros, a fin de combatir el abuso sexual de menores, existe una base de datos nacional para la identificación de las víctimas, o se estaba creando en el momento de la evaluación. Sin embargo, en la mayoría de los Estados miembros, no existe dicha base de datos nacional, o no estaba lo suficientemente desarrollada en el momento de la evaluación. En dichos casos, las fuerzas y cuerpos de seguridad solo utilizan bases de datos y herramientas internacionales, en particular la Base de Datos Internacional sobre Explotación Sexual de Niños de Interpol, una poderosa herramienta de inteligencia e investigación para identificar a las víctimas y a los autores de los delitos, puesto que permite a los investigadores especializados compartir datos en todo el mundo.

- En un Estado miembro, si la policía no es capaz de identificar a la víctima empleando la base de datos, pero tiene sospechas razonables acerca de la posible identidad de un menor, envía una o más fotografías de la víctima a las escuelas para su identificación; esto puede considerarse una buena práctica.

- Los enfoques para luchar contra la revictimización de menores varían entre los Estados miembros: además de bloquear o retirar material de abusos sexuales de menores, es posible incluir en un listado los contenidos peligrosos que se consideran nocivos para los menores, limitar los contactos con el infractor, ofrecer orientación y asesoramiento para las víctimas a través de ONG así como establecer medidas específicas para proteger a las víctimas y a los testigos de abusos sexuales de menores de repercusiones negativas durante los procesos penales.

- En algunos Estados miembros, no se han establecido medidas específicas para evitar la revictimización de menores, pero existe una cooperación a este efecto con ONG, con organismos e instituciones especializados, ajenos a la policía y relacionados con la protección al menor, o con la subprioridad de ciberdelitos «abuso de menores por Internet» del proyecto EMPACT.

- Se han establecido en los Estados miembros diversas medidas jurídicas, técnicas, organizativas e informativas para hacer frente a la explotación o abusos sexuales en línea, al sexteo, al ciberacoso y al turismo sexual que afecta a niños. Varios Estados miembros cuentan con unidades especializadas o con agentes que trabajan exclusivamente con material de abusos sexuales de menores para identificar a los menores y a los autores de los delitos y llevar a cabo investigaciones. En un Estado miembro se somete a los agentes de policía especializados que trabajan en este campo a una evaluación psicológica durante el reclutamiento y, después, de manera anual. Se trata de una buena práctica.

- Todos los Estados miembros han aplicado en distinto grado medidas preventivas con el objetivo de promover el uso seguro de Internet por parte de los menores que, a menudo, han sido elaboradas bajo los auspicios de sus autoridades gubernamentales y en colaboración con las unidades especializadas y con las ONG que trabajan con niños. La UE cofinancia algunos proyectos en este ámbito, como por ejemplo la red INSAFE, en el marco del Programa «Una Internet más Segura» de la Comisión Europea.

- Las medidas de prevención incluyen, entre otras cosas, proyectos de formación y campañas de información destinadas a sensibilizar y formar al público destinatario (estudiantes, padres, educadores y otros colectivos) sobre los principales riesgos potenciales a los que se enfrentan los menores cuando usan Internet, y a desarrollar un uso responsable de este. Las técnicas modernas en que los niños enseñan a los niños, empleadas en un Estado miembro, fueron consideradas buenas prácticas. En algunos Estados miembros, la policía organiza dichas actividades, o participa en ellas.

- La educación sobre los medios de comunicación es también una herramienta poderosa para la prevención de los abusos sexuales de menores, especialmente para los niños y los adolescentes, y en algunos Estados miembros se publica información sobre comportamiento seguro en línea dirigida a los niños en sitios web específicos. Otros Estados miembros han elaborado folletos o manuales o guías pedagógica sobre un uso seguro y eficiente de Internet, el ciberacoso, etc.

- La mayoría de los Estados miembros tiene un servicio de línea directa que puede usarse de manera anónima para denunciar contenidos de abusos sexuales de menores y que a menudo también funciona como una línea directa para niños, adolescentes y padres, en la que se les proporciona asistencia anónima y gratuita, por teléfono y en línea (sitios web o plataformas), y en la que se explica, por ejemplo, cómo presentar una denuncia en la policía. Una plataforma en línea europea (www.reportchildsextourism.eu) reúne todas las líneas nacionales de alerta en Europa.

- La mayoría de los Estados miembros o bien tiene disposiciones que prevén infracciones penales y sanciones para los autores de delitos sexuales contra menores que viajen o bien aplica otras medidas, entre las cuales medidas en contra de la difusión de publicidad sobre oportunidades de cometer abusos y sobre turismo sexual infantil, según prevé el artículo 21 de la Directiva 2011/93/UE. Las medidas encaminadas a mejorar la detección de esta forma específica de delincuencia incluyen sistemas de control o notificación de los viajes de autores de delitos sexuales, acciones conjuntas con el sector del turismo y los viajes y los ministerios de Asuntos Exteriores, el desplazamiento de agentes de enlace al extranjero, la incautación del pasaporte a los autores condenados de delitos sexuales contra menores, etc.

- Las medidas de carácter general para la detección precoz del abuso sexual de menores en Internet incluyen, entre otras cosas, la vigilancia de Internet y la realización de investigaciones encubiertas, herramientas que han demostrado su eficacia para luchar contra la explotación sexual de menores en directo en Internet, así como el uso de herramientas de filtrado que, sin embargo, no se emplean en todos los Estados miembros o no suelen ser obligatorias para los proveedores de servicios de Internet.

- Las medidas coercitivas en casos de abuso sexual de menores en Internet, que incluyen bloquear el acceso a páginas web y retirar sus contenidos o las propias páginas, no se aplican de la misma manera en los Estados miembros, en particular desde el punto de vista procesal, en lo relativo a la necesidad de contar con una orden judicial antes de actuar o a modo de confirmación de las medidas adoptadas por la policía.

- En la mayoría de los Estados miembros se adoptan medidas legales y prácticas para retirar permanentemente de la red material audiovisual de abusos sexuales de menores. Puede optarse por el «enfoque de supresión», pero de este modo no se impide que las imágenes o los vídeos de menores sigan mostrándose en otros sitios de Internet. Otros Estados miembros utilizan también, o exclusivamente, el «enfoque de bloqueo del acceso», que consiste en bloquear el acceso a los sitios web que contienen material pornográfico infantil volviéndolo así temporalmente inaccesible.

- Si el material está alojado en servidores situados en el extranjero, se emplean por lo general canales internacionales, a saber, Europol y su sistema seguro de intercambio de información SIENA o Interpol y su iniciativa de bloqueo del acceso; también es posible que las líneas directas informen simultáneamente a INHOPE (Asociación Internacional de Líneas Directas de Denuncia de Internet), lo que garantiza que el material de abuso sexual de menores dirigido a un Estado pero almacenado en el extranjero pueda ser eliminado de Internet.

- En algunos Estados miembros se bloquea e imposibilita el acceso a sitios web con material de abuso sexual de menores sin importar si el sitio está alojado dentro o fuera de la UE, algo que se consideró una buena práctica.

- Para la aplicación de las medidas anteriormente mencionadas, es esencial que exista una buena cooperación entre todas las partes interesadas pertinentes, a saber, las fuerzas y cuerpos de seguridad, las líneas directas, las ONG y los proveedores de servicios de Internet. En algunos Estados miembros, estos últimos tienen la obligación de adoptar medidas adecuadas para acabar con la posibilidad de utilizar dicho material, ya sea bloqueando el acceso o eliminando el contenido de Internet, mientras que en otros Estados miembros la legislación nacional no estipula una obligación de este tipo, aunque las medidas anteriormente mencionadas pueden adoptarse en casos individuales sobre la base de una orden judicial.

- La cooperación en los Estados miembros entre las fuerzas y cuerpos de seguridad y los proveedores nacionales de servicios de Internet es, en general, buena, y a menudo estos retiran material de abuso sexual de menores rápida y voluntariamente tras recibir notificación de las fuerzas y cuerpos de seguridad, incluso cuando no tienen la obligación de hacerlo. Se mencionó como ejemplo de buena práctica una herramienta empleada en un Estado miembro: un mismo icono de la interfaz para todos los proveedores, con un botón de alerta que puede pulsarse para denunciar que un sitio web contiene material de abuso sexual de menores.

RECOMENDACIONES

- ***Los Estados miembros que aún no lo hayan hecho, deben elaborar una base de datos nacional dedicada a la identificación de las víctimas para luchar contra el abuso sexual de menores o facilitar el acceso a la base de datos de Interpol. Los Estados miembros deben también considerar la creación de una red nacional para compartir la información sobre la identificación de las víctimas.***

- ***Los Estados miembros que aún no lo hayan hecho deben considerar la concepción de medidas específicas para evitar la revictimización de los menores, en particular medidas para proteger a las víctimas y testigos de abusos sexuales de menores de las consecuencias negativas durante los procesos penales.***

- ***Los Estados miembros deben garantizar el buen funcionamiento de la cooperación entre todos los agentes pertinentes, a fin de combatir de manera eficaz los delitos que tienen como objeto a menores en Internet, y considerar la instauración de la obligación por parte de los proveedores de servicios de adoptar medidas adecuadas, como bloquear el acceso, suprimir los contenidos y retirar los sitios web.***

XVI -MECANISMO PARA RESPONDER A LOS CIBERATAQUES

CONCLUSIONES Y RECOMENDACIONES CLAVE

- En el momento de la evaluación, la Directiva 2013/40/UE del Parlamento Europeo y del Consejo, de 12 de agosto de 2013, relativa a los ataques contra los sistemas de información había sido incorporada al ordenamiento jurídico de la mayoría de los Estados miembros. El estado actual de la incorporación de dicha Directiva a las diferentes legislaciones nacionales se puede consultar en: http://eur-lex.europa.eu/legal-content/EN/NIM/?uri=celex:32011L0093

- Los ciberataques constituyen una amenaza cambiante, los métodos y herramientas de los que se sirven dichos ataques cada vez son más sofisticados y el espectro de la amenaza de los ciberataques en el ciberespacio es muy amplio. En concreto, la evaluación ha mostrado que han aumentado de forma significativa los ataques «con programas de secuestro de datos» (*ransomware*), un tipo de programa malintencionado que bloquea el acceso a los datos hasta que se paga un rescate.

- Algunos Estados miembros cuentan con la asistencia técnica del sector privado en los casos de ciberataques, dado que las sociedades privadas poseen buenos conocimientos técnicos y trabajan con mejores equipos y menos costes. Por otra parte, pueden ayudar a evaluar las consecuencias de los ataques a las infraestructuras y a obtener un conocimiento global de la situación.

- En algunos Estados miembros ya existe un planteamiento multiinstitucional basado, en ciertos casos, en asociaciones público-privadas, mientras que en otros Estados miembros un planteamiento de ese tipo o bien no se ha desarrollado de forma suficiente o bien es inexistente y los mecanismos de coordinación para reaccionar a los ciberataques funcionan principalmente sobre la base de una cooperación informal.

- En el momento en que se efectuó la evaluación, la mayoría de los Estados miembros ya habían creado a nivel nacional un equipo de respuesta a incidentes de seguridad informática (siglas inglesas CSIRT) o lo estaban creando, mientras que unos pocos Estados miembros todavía no lo habían hecho.

- Las funciones principales de los CSIRT son: supervisar y responder a los incidentes cibernéticos, emitir alertas tempranas y advertencias y realizar análisis de riesgos e incidentes, así como establecer la cooperación con el sector privado.

- En algunos Estados miembros el papel de los CSIRT nacionales sobrepasa incluso estas tareas, pues gestionan las bases de datos sobre amenazas e incidentes, apoyan el intercambio de información entre varios organismos, proporcionan asesoría y asistencia para la protección de los sistemas informáticos del sector público y privado, emprenden actividades anticipatorias para disminuir los riesgos de incidentes en el campo de la seguridad informática, efectúan actividades de sensibilización y formación, actúan como intermediarios entre el sector privado, las instituciones universitarias y la policía y representan al punto de contacto nacional en la cooperación internacional.

- Los CSIRT gubernamentales gestionan principalmente las crisis y proporcionan una respuesta a las amenazas e incidentes cibernéticos del sector público, pero en muchos casos también cuando se producen en infraestructuras críticas, y en casos limitados, incluso en el sector privado, pese a que normalmente esto corresponde a los demás CSIRT del sector privado.

- En algunos Estados miembros, los CSIRT gubernamentales ejercen funciones de coordinación y supervisión para otros agentes pertinentes, lo que resulta una práctica normal, especialmente en aquellos Estados miembros en los que el mecanismo de respuesta a los ciberataques es bastante complejo o en los que coexisten en paralelo un número considerable de diferentes CSIRT en los sectores privado y público.

- Los CSIRT no tienen las competencias de los cuerpos o fuerzas de seguridad de cara a las personas, pero respecto a ataques de naturaleza penal (no todos los incidentes cibernéticos son actos delictivos), desempeñan un papel importante a la hora de apoyar las investigaciones, ya que pueden ayudar a proporcionar información y a asegurar las pruebas electrónicas. Por ello, desde este punto de vista, es importante que los CSIRT mantengan una buena cooperación con los cuerpos o fuerzas de seguridad, pues, dado que los datos son muy dinámicos y pueden perderse fácilmente, la obtención efectiva de la información y de las pruebas es esencial para la investigación de los ciberataques. Si es necesario, en las investigaciones de los ciberincidentes pueden participar servicios de inteligencia.

- De conformidad con la Directiva UE 2016/1148 (Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (Directiva SRI)), que tiene que ser incorporada a las legislaciones nacionales a más tardar el 9 de mayo de 2018, los Estados miembros deben crear CSIRT que funcionen bien y cumplan con determinados requisitos para garantizar que puedan tratar eficazmente los incidentes y riesgos, y establecer una cooperación eficaz a nivel de la UE.

- Solos, los gobiernos no pueden llegar a adquirir la resiliencia digital; al sector privado también le corresponde un papel importante, en particular a los operadores de servicios esenciales, los operadores de sistemas y los operadores redes de información, que participan directamente en la gestión de riesgos y en la protección de la seguridad de sus redes y servicios.

- Con arreglo a la Directiva SRI, los Estados miembros garantizarán que los operadores de servicios esenciales protejan la seguridad de sus redes y sistemas de información y que notifiquen, sin demora indebida, a la autoridad competente o a los CSIRT cualquier incidente que tenga un impacto importante sobre la prestación del servicio. Por consiguiente, una vez que se haya pasado a la plena aplicación de la Directiva SRI, las entidades que cumplan los criterios de la definición de operador de servicios esenciales estarán obligadas por ley a notificar los incidentes que tengan efectos significativos en la continuidad del servicio esencial que prestan.

- En algunos casos, a falta de una obligación formal, la notificación se efectuaba con carácter voluntario; no obstante, como se ha puesto de relieven en algunos informes, es frecuente la falta de notificación debido a la renuencia de los proveedores de servicios que temen que su reputación se vea perjudicada. Como concluye la evaluación, si no hay una obligación de notificación se corre el peligro real de que la mayor parte de los casos de incidentes cibernéticos escape al conocimiento de las autoridades. Como se ha puesto de relieve en uno de los informes particulares, para fomentar que se notifiquen los incidentes, las autoridades policiales pueden hacer hincapié en que la investigación se puede llevar a cabo de forma secreta y se pueden lograr buenos resultados sin afectar a la reputación de los proveedores.

- Como concluye la evaluación, si no hay una obligación de notificación se corre el peligro real de que la mayor parte de los casos de incidentes cibernéticos escape al conocimiento de las autoridades.

- Un sistema obligatorio de notificación, especialmente de los delitos graves, no solo es importante a efectos policiales, es decir, para facilitar una evaluación acelerada y completa de la situación y una aplicación más rápida de las contramedidas apropiadas, sino que también es útil para proporcionar a las autoridades una visión general más exacta de las amenazas, recopilar estadísticas generales del número de incidentes de ciberseguridad y adoptar medidas cautelares adecuadas. Por todo ello, los evaluadores han considerado que sería una buena práctica establecer un marco jurídico adecuado que hiciese obligatoria dicha notificación, como ocurre en algunos Estados miembros.

- Para garantizar un alto nivel de ciberseguridad, es necesario que se cree una concienciación en torno a la seguridad entre los dirigentes, desarrolladores de sistemas y usuarios, que mejore la seguridad; por eso, la sensibilización a todos los niveles, como se ha hecho en determinados Estados miembros, es un elemento importante de un planteamiento eficaz de la ciberseguridad.

- Como a veces las amenazas y ataques cibernéticos tienen una dimensión transfronteriza, la sección de ciberataques de EMPACT ha resultado una plataforma útil para mejorar la cooperación entre los Estados miembros, las instituciones y organismos pertinentes y los socios del sector privado a la hora de producir y divulgar programas antiprogramas maliciosos («antimalware») y programas de defensa contra los ataques en redes a infraestructuras.

- Vale la pena mencionar la estrecha cooperación entre los CSIRT de los tres Estados Bálticos, los cuales en noviembre de 2015 firmaron un memorando de entendimiento comprometiéndose a intensificar la cooperación sobre ciberseguridad y protección de los sistemas y redes informáticos.

- Cuando se trata de ciberataques fuera de la UE, se utilizan los cauces formales de la asistencia judicial. No obstante, como el aspecto temporal en lo referente a los ciberdelitos puede ser fundamental (debido a la volatilidad de los datos), también se recurre a la cooperación directa y al intercambio de información entre las fuerzas policiales directamente o a través de Europol e Interpol para que la cooperación sea más rápida y eficaz. Algunos Estados miembros también utilizan la red de puntos de contacto del G7 de servicio ininterrumpido.

- La Agenda Digital para Europa incentivaba a los Estados miembros a crear, antes de 2012, una red de CSIRT que funcione bien a nivel nacional para cubrir toda Europa. La Comisión Europea ha invitado a los Estados miembros a reforzar la cooperación entre los CSIRT nacionales existentes y a ampliar los mecanismos de cooperación vigentes, como el grupo europeo de CSIRT gubernamentales.

- La comunicación y cooperación también se llevan a cabo a nivel internacional a través de las redes de CSIRT que se han formado en todo el mundo, como la Red internacional de vigilancia y alerta, FIRST, la red europea de CSIRT gubernamentales y los TF-CSIRT, con el objeto de cooperar sobre incidentes cibernéticos, en particular para apoyarse mutuamente en la gestión de asuntos informáticos y en la gestión de crisis informáticas, pues ellos efectúan estos ejercicios de manera regular. Las redes de CSIRT pueden compartir parcialmente intereses similares, por ejemplo los CSIRT gubernamentales y de determinadas autoridades, y parcialmente intereses diferentes, por ejemplo con equipos procedentes de empresas, de la ciencia y de otras autoridades.

RECOMENDACIONES

- ***Para garantizar un nivel apropiado de protección y seguridad del ciberespacio nacional, los Estados miembros deben establecer un marco institucional eficiente, basado en un planteamiento multiinstitucional y que comporte una cooperación adecuada entre todos los agentes pertinentes que participan en la ciberseguridad, incluido, en su caso, el sector privado.***

- ***De conformidad con la Directiva SRI, los Estados miembros que aún no lo han hecho deben crear un* CSIRT *nacional***. Para garantizar un alto nivel de ciberseguridad, los Estados miembros deben considerar conferir a los CSIRT gubernamentales funciones que les permitan actuar como puntos centrales de coordinación de otros CSIRT y agentes que participan en la prevención de las ciberamenazas y en las respuestas a los incidentes de ciberseguridad.

- ***Para ello, los Estados miembros deben también considerar encomendar a los* CSIRT *gubernamentales tareas como la recopilación y el análisis de ciberincidentes, el desarrollo de su capacidad para responder a las amenazas y de sistemas informáticos de alerta rápida, y proporcionar formación específica sobre ciberdelincuencia y ciberseguridad***.

- ***De acuerdo con la Directiva SRI, los Estados miembros garantizarán que los operadores de servicios esenciales notifiquen sin demora indebida cualquier ciberincidente que tenga efectos significativos en la continuidad de los servicios esenciales que prestan.***

- ***Se anima a los Estados miembros a que participen en la sección de ciberataques de la plataforma EMPACT, así como en la red de* CSIRT *conforme a lo dispuesto en la Directiva SRI, y en otras redes de este tipo, según proceda***.

XVII - COOPERACIÓN CON ORGANISMOS DE LA UE

CONCLUSIONES Y RECOMENDACIONES CLAVE

- Dado que en la ciberdelincuencia en sentido estricto y delincuencia favorecida por el ámbito cibernético, así como en su investigación, participan con frecuencia varios Estados miembros, la cooperación y el intercambio de información con los organismos de la UE es fundamental.

- Europol/EC3, Eurojust, la Red Judicial Europea y la ENISA desempeñan un papel clave en una amplia gama de actividades, como la elaboración de análisis de las tendencias de la ciberdelincuencia, la coordinación de las investigaciones y acciones penales internacionales, el intercambio de información, la inteligencia criminal, las pruebas y el análisis de datos y la contribución formación a escala de la UE. Su conocimiento y sus medios permiten la cooperación mutua entre los Estados miembros y sus fuerzas o cuerpos de seguridad y ministerios fiscales respectivos.

- Eurojust desempeña un papel importante en la coordinación de las investigaciones y acciones penales internacionales y en la oferta de asistencia judicial respecto de la cooperación transfronteriza y la transferencia de pruebas entre los Estados miembros, algo que resulta especialmente útil en los casos de ciberdelitos complejos. Asimismo, contribuye a facilitar y acelerar la cooperación con las autoridades competentes de los Estados miembros y de los terceros países en el ámbito de la ciberdelincuencia.

- Eurojust también recopila y difunde estudios de casos y buenas prácticas, contribuye a las actividades de formación en el ámbito de la ciberdelincuencia y fomenta el intercambio de experiencias entre los fiscales y los jueces especializados en el ámbito de la ciberdelincuencia, en particular a través del apoyo a la Red judicial europea sobre ciberdelincuencia.

- Europol facilita la cooperación y el intercambio de información entre los Estados miembros, distribuye productos y servicios operativos a los servicios de investigación y ofrece formación criminalística y operativa y material de sensibilización. El Centro Europeo de Ciberdelincuencia (EC3) pretende reforzar la respuesta policial a la ciberdelincuencia en la UE y así contribuir a la protección de los ciudadanos, las empresas y las administraciones públicas de Europa frente a la delincuencia en la red. El EC3 presta asistencia operativa e investigativa a los servicios de investigación de la ciberdelincuencia nacionales en tres áreas principales: el fraude en línea, la explotación sexual de menores en línea y los ciberataques contra infraestructuras vitales y sistemas informáticos de la Unión Europea. Estas actividades cuentan con el apoyo del Equipo de inteligencia cibernética (siglas inglesas CIT), cuyos analistas recogen y tratan información relacionada con los delitos cibernéticos procedente de fuentes públicas, privadas y abiertas, y detectan las nuevas amenazas y pautas de acción. Junto con el EC3 trabaja el Grupo especial conjunto de acción contra los delitos cibernéticos (siglas inglesas J-CAT), que se ocupa de los casos más importantes a escala internacional que afectan a los Estados miembros y sus ciudadanos. La experiencia operativa muestra el valor añadido que reviste la pronta intervención de los funcionarios de enlace especializados del J-CAT en la coordinación de las principales operaciones contra el delito cibernético.

- Los Estados miembros aprecian en general el apoyo y la coordinación que ofrecen Europol/EC3, Eurojust, la Red Judicial Europea con ayuda de sus puntos de contacto, y consideran que su función es fundamental para aumentar la confianza mutua entre las autoridades encargadas de la investigación y las fiscalías, así como para facilitar la cooperación internacional también con terceros Estados.

- El papel de la ENISA en la recogida y transmisión de las ciberalertas mediante sistemas automatizados también está contribuyendo notablemente a reforzar la seguridad técnica de los sistemas de información.

- No obstante, ni los servicios ni los productos que Europol, Eurojust, la Red Judicial Europea y la ENISA pueden ofrecer en relación con la ciberdelincuencia son siempre conocidos del todo, por lo que los profesionales del ramo de los Estados miembros no los aprovechan al máximo.

RECOMENDACIONES

- ***Los Estados miembros deben aprovechar al máximo los servicios y productos que ofrecen Eurojust, la Red Judicial Europea y Europol con respecto a la ciberdelincuencia, y facilitar una estrecha cooperación entre sus CSIRT nacionales y la ENISA.***

- ***Eurojust, Europol y la ENISA deben considerar el fomento de la concienciación sobre sus servicios y las posibilidades existentes para la cooperación y la formación especializada que ellos ofrecen en el ámbito de la ciberdelincuencia, y apoyar activamente iniciativas que refuercen la cooperación internacional en lo que se refiere a la lucha contra la ciberdelincuencia.***

- ***Europol también debe aprovechar el despliegue del sistema SIENA en los servicios de investigación, mejorar la visibilidad de los proyectos EMPACT, explorar el mejor uso posible del J-CAT, considerar proponer a los Estados miembros un enfoque normalizado sobre elementos estructurales de las bases de datos dedicadas a la inteligencia criminal sobre ciberdelincuencia, y facilitar la adopción de una taxonomía común sobre ciberdelincuencia.***

- ***La ENISA debe estudiar la manera de normalizar el concepto de las ciberalertas que se recogen y transmiten mediante sistemas automatizados, lo que haría posible que las estadísticas sobre estas alertas fueran comparables entre sí y estuvieran armonizadas en todos los Estados miembros.***

XVIII - EQUIPOS CONJUNTOS DE INVESTIGACIÓN (ECI)

CONCLUSIONES Y RECOMENDACIONES CLAVE

- Debido a que con mucha frecuencia la ciberdelincuencia tiene una dimensión transfronteriza, la participación en investigaciones coordinadas internacionalmente puede ser beneficiosa para procesar eficazmente los delitos cibernéticos.

- En el marco de la UE, los equipos conjuntos de investigación (ECI) son un instrumento de cooperación internacional en los casos de delincuencia transnacional, basados en un acuerdo entre las autoridades competentes de dos o más Estados miembros (tanto de autoridades judiciales como policiales) con el fin de llevar a cabo de manera conjunta las investigaciones penales.

- En el momento de la evaluación, varios Estados miembros habían participado en un ECI en relación con ciberdelitos, algunos con más frecuencia que otros, mientras que otros Estados miembros nunca lo habían hecho.

- La participación en un ECI se percibe generalmente como una experiencia positiva por parte de los Estados miembros participantes, los cuales consideran que los ECI son un instrumento eficaz para llevar a cabo investigaciones transfronterizas, que permiten el intercambio directo de información entre los investigadores y la recogida transfronteriza y oportuna de pruebas sin tener que presentar por separado solicitudes formales de asistencia judicial.

- Debido a los dilatados procedimientos que acarrea la asistencia judicial, la utilización de los ECI contribuye a reducir los plazos de las investigaciones y a mejorar, además, la confianza entre las autoridades nacionales.

- Aunque la participación de Europol y Eurojust en la creación de estos equipos no es obligatoria, como indican algunos Estados miembros, ambas agencias pueden desempeñar un papel importante a la hora de garantizar la eficacia y la capacidad operativa de los ECI. Algunos Estados miembros consideran fundamental la posibilidad de que los ECI sean financiados por Eurojust y Europol.

RECOMENDACIONES
• ***Se exhorta a los Estados miembros a que conciencien a los profesionales sobre las posibilidades y ventajas de los ECI y su utilización en los casos de ciberdelito, con el fin de que las investigaciones sean más eficaces.***   • ***Las instituciones, agencias y organismos de la UE, en particular Eurojust y Europol, deben seguir apoyando y facilitando la creación de ECI y facilitar una financiación adecuada para ayudar a los Estados miembros a recurrir con mayor frecuencia a estos equipos.***

XIX - ASISTENCIA JUDICIAL

CONCLUSIONES Y RECOMENDACIONES CLAVE

- Debido a su carácter predominantemente transnacional, para luchar contra el delito cibernético suele ser precisa una cooperación internacional fluida y eficiente, así como el recurso a la asistencia judicial.

- La legislación nacional de los Estados miembros no contiene disposiciones específicas sobre las solicitudes de asistencia judicial en los casos de ciberdelito y, por consiguiente, son de aplicación los procedimientos y condiciones generales de la asistencia judicial.

- La mayoría de los Estados miembros son Partes del Convenio Europeo de Asistencia Judicial en Materia Penal celebrado entre los Estados miembros de la Unión Europea, de 29 de mayo de 2000 (Convenio de Asistencia Judicial), de conformidad con el artículo 34 del Tratado de la Unión Europea, y su Protocolo adicional de 2001. También participan en Schengen y aplican su acervo, por el que son aplicables también las disposiciones sobre cooperación judicial del Convenio de Schengen, algo que es de importancia en el caso de los Estados miembros que no son Partes en el Convenio de Asistencia Judicial. En cuanto a los Estados que no son Partes en los citados acuerdos multilaterales, ni en convenios bilaterales, la asistencia judicial se basa el principio de reciprocidad.

- Las solicitudes judiciales de asistencia judicial van precedidas generalmente de solicitudes de que se protejan con rapidez las pruebas electrónicas almacenadas en los datos del sistema informático, como establece el artículo 29 del Convenio de Budapest sobre la Ciberdelincuencia, de 22 de noviembre de 2001.

- El plazo para responder a una solicitud de asistencia judicial puede llegar a algunos meses, pero varía según las diferentes circunstancias, por ejemplo en función de si la asistencia se proporciona con arreglo a un acuerdo internacional o al principio de reciprocidad; en este último caso, el tiempo de respuesta es aún mayor pues, en primer lugar, es necesario recibir o conceder una garantía de reciprocidad.

- Ante la rápida evolución de la ciberdelincuencia, la lentitud de los procedimientos de asistencia judicial hace que sean bastante ineficaces, y que esto acarree consecuencias negativas para el desarrollo y el éxito de las investigaciones, dado que las pruebas electrónicas son precarias y cualquier retraso puede dar lugar a la pérdida de los datos. En consecuencia es necesario en general acelerar la tramitación de las solicitudes de asistencia judicial en las investigaciones de los ciberdelitos. La mejora de la calidad de las solicitudes de asistencia judicial puede suponer que se acelere notablemente su ejecución en otros países.

- Como alternativa a los canales formales de la asistencia judicial, algunos Estados miembros utilizan los canales de Europol, Eurojust y de la Red Judicial Europea, como el J-CAT en el EC3 o Interpol, la red de puntos de contacto del G7, las redes de los funcionarios de enlace o los contactos bilaterales, para obtener una respuesta más rápida; no obstante, hay que tener en cuenta que, en caso de que se utilicen estos canales menos formales, se tendría que verificar la admisibilidad de los datos como pruebas ante los tribunales.

- Se considera muy útil el apoyo de Eurojust a la hora de facilitar la comunicación y acelerar la ejecución de las solicitudes urgentes no solo cursadas a los Estados miembros o recibidas de ellos, sino también con terceros países, así como la presencia física de los fiscales de enlace de los Estados Unidos, Noruega y Suiza en Eurojust.

- Como se indica en numerosos informes individuales, muchas de las solicitudes de asistencia judicial relacionadas con el ciberdelito van dirigidas a la obtención de pruebas materiales que están en posesión de los proveedores de servicios. Como muchos de estos están bajo la jurisdicción de los EE.UU., por lo que se refiere a los países no pertenecientes a la UE, la asistencia judicial en asuntos penales referentes a ciberdelitos se solicita principalmente a los EE.UU. y por ello es fundamental una cooperación fluida con ese país.

- A pesar de ello, muchos Estados miembros encuentran dificultades a este respecto, en particular por lo que se refiere a la conservación y divulgación de los datos relativos a las direcciones IP de los titulares de cuentas de Facebook y otras redes sociales. Como han señalado los evaluadores en algunos informes individuales, la cuestión de la accesibilidad a las bases de datos de las redes sociales originarias de los EE.UU. es un problema que afecta a todos los Estados miembros.

- En general los EE.UU. imponen requisitos formales y de contenido muy estrictos a dichas solicitudes, en particular por lo que se refiere a la relación entre el delito y el elemento específico de la prueba que es objeto de la solicitud de transmisión.

- Según los resultados de la evaluación, resultaría útil llegar a adoptar soluciones internacionales para mejorar los procedimientos de asistencia judicial con terceros Estados, como los EE.UU. El uso de un formulario para las solicitudes de requerimientos de presentación rápida acordados por las autoridades de ejecución en un Estado determinado se puede considerar como una buena práctica.

- Conforme a lo dispuesto en el Derecho estadounidense, para la búsqueda de una localización o la obtención de los datos de correo electrónico o de cualquier contenido de una comunicación almacenada por un proveedor de servicios, es necesaria una resolución judicial denominada «orden de registro», lo cual podría satisfacer el criterio de la «causa probable». Este procedimiento es muy largo y, en muchos casos, no da lugar a la ejecución de la solicitud.

- Algunos Estados miembros han reconocido que los contactos informales y personales con las autoridades competentes de terceros Estados antes del envío de una solicitud de asistencia judicial han resultado de gran utilidad para garantizar una mejor y más rápida ejecución de dichas solicitudes.

- La creación de sistemas de registro y de gestión de la asistencia judicial haría posible seguir un asunto desde el registro hasta el envío de la respuesta al país solicitante, y por ello puede considerarse una buena práctica.

RECOMENDACIONES

- ***Los Estados miembros deben explorar las vías para seguir mejorando la calidad de las solicitudes de asistencia judicial que envíen a otros países, en particular asegurarse de que estén debidamente cumplimentadas y estudiar las maneras de acelerar y mejorar la calidad de las respuestas a las solicitudes de asistencia judicial.***

- ***Se recomienda a los Estados miembros que refuercen la eficacia del proceso de comunicación con otros Estados miembros y terceros países y consideren la instauración de métodos para seguir un asunto desde su registro hasta el envío de la respuesta al país solicitante como, a modo de ejemplo, un sistema de registro de la asistencia judicial.***

- ***Se exhorta a los Estados miembros a que utilicen en mayor medida los instrumentos de Eurojust, la Red Judicial Europea y Europol, y a que mantengan contactos informales con las autoridades competentes de terceros países a fin de obtener respuestas más rápidas a las solicitudes de asistencia judicial procedentes de ellos.***

- ***La UE debe seguir trabajando a fin de encontrar soluciones para mejorar y acelerar la comunicación entre los Estados miembros y terceros países, en particular los EE.UU., especialmente en lo que se refiere al intercambio de información operativa y a la ejecución de las solicitudes de asistencia judicial.***

- ***La UE debe considerar la creación de un marco para la cooperación directa con los proveedores pertinentes de servicios no pertenecientes a la UE.***

XX — FORMACIÓN

CONCLUSIONES Y RECOMENDACIONES CLAVE

- Teniendo en cuenta el rápido avance tecnológico y el carácter cambiante de la ciberdelincuencia, y por consiguiente la necesidad de adaptarse a las nuevas tendencias y *modus operandi* más sofisticados, para el éxito de las investigaciones y de los procesamientos de la ciberdelincuencia en sentido estricto y la delincuencia favorecida por el ámbito cibernético, es de crucial importancia la formación especializada regular y continua sobre ciberdelincuencia y ciberseguridad de los profesionales a todos los niveles, inclusive al principio de sus carreras.

- En la mayoría de los Estados miembros se están realizando importantes esfuerzos, en medios y personal, en formación para las fuerzas y cuerpos de seguridad especializada en el ámbito de la ciberdelincuencia, si bien no todos los Estados miembros poseen el mismo nivel de formación de la judicatura y en algunos Estados miembros, aunque exista este tipo de formación, no es obligatoria.

- No obstante, habida cuenta de las especificidades técnicas de la ciberdelincuencia, se requiere un alto grado de conocimiento por parte no solo de las fuerzas y cuerpos de seguridad sino también de los jueces que presiden los asuntos; del mismo modo, es fundamental que los cuerpos policiales, fiscales y jueces que se ocupen del ciberdelito reciban formación especializada que comprenda la recogida, el análisis y el uso de las pruebas electrónicas.

- En algunos Estados miembros, además de la formación impartida por los organismos públicos (academias o institutos policiales o judiciales, etc.), también facilitan formación organismos externos, como universidades y empresas privadas o también ONG que operan en el sector, cuyo conocimiento técnico resulta muy útil para una formación de buena calidad. Algunos Estados miembros han creado centros de excelencia altamente especializados que imparten formación sobre ciberdelincuencia.

- En algunos Estados miembros, la formación también se proporciona en forma de sesiones de aprendizaje a distancia, de formación por internet o también con archivos multimedia; estos medios pueden considerarse buenas prácticas y un método de formación efectivo.

- Además de la formación impartida a nivel nacional, también los órganos pertinentes de la UE, a saber, el Centro Europeo de Ciberdelincuencia/Europol, ECTEG (Grupo Europeo de Formación y Educación en Ciberdelincuencia), Eurojust, la OLAF, la CEPOL y la ENISA, imparten formación especializada en el ámbito de la ciberdelincuencia, o contribuyen a dicha formación; sin embargo, los Estados miembros no suelen utilizar en toda su potencialidad estas posibilidades.

- Algunos Estados miembros disponen de un presupuesto específico destinado a la formación en materia de ciberdelincuencia. En algunos Estados miembros deberían hacerse esfuerzos adicionales para mejorar la formación especializada en ciberdelincuencia que se imparte a todas las categorías de funcionarios que participan en los casos de ciberdelincuencia.

- Según los resultados de la evaluación, un enfoque integrado para la formación de los jueces, los fiscales y los cuerpos y fuerzas de seguridad puede contribuir a mejorar los conocimientos sobre ciberdelincuencia y funcionar como una plataforma para el intercambio de experiencias y buenas prácticas por lo que respecta a la ciberdelincuencia y para debatir los obstáculos relacionados con la admisibilidad de las pruebas. A pesar de ello, la evaluación recíproca ha puesto de relieve que solo unos pocos Estados miembros ya ofrecen este tipo de formación conjunta.

RECOMENDACIONES

- ***Los Estados miembros deben ofrecer una amplia formación que abarque el proceso completo de la ciberdelincuencia y que vaya destinada a todas las partes interesadas y a los profesionales que participan en la lucha contra la ciberdelincuencia, y en particular una formación más periódica destinada a la judicatura, y estudiar la posibilidad de asignar un presupuesto específico a la formación en materia de ciberdelincuencia.***

- ***Los Estados miembros deben considerar la organización de formación conjunta en materia de ciberdelincuencia para las fuerzas y cuerpos de seguridad, los fiscales y los jueces, así como la utilización del aprendizaje por medios informáticos.***

- ***Los Estados miembros deben aprovechar mejor las oportunidades de formación proporcionadas tanto por los organismos de la UE, como el EC3/Europol, ECTEG, Eurojust, OLAF, CEPOL y ENISA, como las ofrecidas por las instituciones académicas y las empresas privadas, y considerar la creación de centros de excelencia que impartan formación específica sobre ciberdelincuencia.***

- ***Las instituciones de la UE deben aumentar la financiación de la UE destinada a ayudar a los Estados miembros a organizar más cursos de formación especializada sobre ciberdelincuencia para los profesionales nacionales.***