Naciones Unidas E/CN.15/2018/6

Consejo Económico y Social

Distr. general
22 de febrero de 2018
Español
Original: inglés

Comisión de Prevención del Delito y Justicia Penal
27º período de sesiones
Viena, 14 a 18 de mayo de 2018
Tema 5 del programa provisional*
Debate temático sobre las respuestas de la justicia penal para prevenir y combatir la ciberdelincuencia en todas sus formas, en particular mediante el fortalecimiento de la cooperación en los planos nacional e internacional

Guía para el debate temático sobre las respuestas de la justicia penal para prevenir y combatir la ciberdelincuencia en todas sus formas, en particular mediante el fortalecimiento de la cooperación en los planos nacional e internacional

Nota de la Secretaría

Resumen

La presente guía para el debate temático sobre las respuestas de la justicia penal para prevenir y combatir la ciberdelincuencia en todas sus formas, en particular mediante el fortalecimiento de la cooperación en los planos nacional e internacional, que se celebrará durante el 27º período de sesiones de la Comisión de Prevención del Delito y Justicia Penal, ha sido preparada por la Secretaría con arreglo a lo dispuesto en la decisión 18/1 de la Comisión. En su decisión 2016/241, el Consejo Económico y Social decidió que el tema principal del 27º período de sesiones de la Comisión se titularía “Respuestas de la justicia penal para prevenir y combatir la ciberdelincuencia en todas sus formas, en particular mediante el fortalecimiento de la cooperación en los planos nacional e internacional”. En la presente nota, se proponen varias cuestiones sobre las esferas temáticas pertinentes para el debate temático, se plantean algunas cuestiones a fin de estructurarlo y se proporciona información de antecedentes.

* E/CN.15/2018/1.

V.18-00976 (S) 190318 190318

I. Introducción

1. En su decisión 2016/241, el Consejo Económico y Social decidió que el tema principal del 27º período de sesiones de la Comisión de Prevención del Delito y Justicia Penal se titularía “Respuestas de la justicia penal para prevenir y combatir la ciberdelincuencia en todas sus formas, en particular mediante el fortalecimiento de la cooperación en los planos nacional e internacional”.

2. En la continuación de su 26º período de sesiones, celebrada los días 7 y 8 de diciembre de 2017, la Comisión aprobó la propuesta del Presidente sobre el enfoque relativo a la organización del debate temático en su 27º período de sesiones que figura a continuación: el debate temático se celebraría durante una sesión de mañana y una sesión de tarde. El debate de la mañana se dedicaría al subtema relativo a las dificultades actuales, y el debate de la tarde al subtema relativo a las posibles respuestas.

3. La Secretaría ha preparado la presente nota de conformidad con la decisión 18/1, titulada “Directrices para los debates temáticos de la Comisión de Prevención del Delito y Justicia Penal”, en la que la Comisión decidió que el debate sobre el tema principal se basaría en una guía para los debates, incluida una lista de cuestiones que habrían de abordar los participantes.

II. Información de antecedentes: sentar las bases para el debate temático

4. Si bien el rápido crecimiento de Internet y la tecnología informática ha transformado a las sociedades de todo el mundo, también ha creado nuevas oportunidades para la delincuencia. Las computadoras, las redes y los datos pueden vincularse a diversas formas de delincuencia de casi cualquier manera concebible. Han pasado a ser a la vez objeto de delito e instrumentos del delito y han dado lugar a nuevos motivos y oportunidades para la expansión de la delincuencia. Con frecuencia inclinan la balanza de riesgos y recompensas para los delincuentes en favor de las últimas. Además, como consecuencia de la arquitectura digital básica de Internet y la disponibilidad mundial de las tecnologías de la información y las comunicaciones (TIC), la ciberdelincuencia tiene vínculos con la delincuencia organizada y suele ser de carácter transnacional[1].

5. En su resolución 65/230, la Asamblea General hizo suya la Declaración de Salvador sobre Estrategias Amplias ante Problemas Globales: los Sistemas de Prevención del Delito y Justicia Penal y su Desarrollo en un Mundo en Evolución, aprobada en el 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, y solicitó a la Comisión de Prevención del Delito y Justicia Penal que estableciera, con arreglo a lo dispuesto en el párrafo 42 de la Declaración de Salvador, un grupo intergubernamental de expertos de composición abierta para que realizara un estudio exhaustivo del problema del delito cibernético y las respuestas de los Estados Miembros, la comunidad internacional y el sector privado ante ese fenómeno, incluido el intercambio de información sobre legislación nacional, mejores prácticas, asistencia técnica y cooperación internacional, con miras a examinar opciones para fortalecer las actuales respuestas jurídicas o de otra índole ante el delito cibernético en los planos nacional e internacional y proponer otras nuevas.

6. Se renovó ese mandato en la Declaración de Doha sobre la Integración de la Prevención del Delito y la Justicia Penal en el Marco Más Amplio del Programa de las Naciones Unidas para Abordar los Problemas Sociales y Económicos y Promover el Estado de Derecho a Nivel Nacional e Internacional y la Participación Pública, aprobada

[1] *The Globalization of Crime: A Transnational Organized Crime Threat Assessment* (publicación de las Naciones Unidas, núm. de venta E.10.IV.6), pág. 204; e *Informe Mundial sobre las Drogas 2017:* El problema de las drogas y la delincuencia organizada, las corrientes financieras ilícitas, la corrupción y el terrorismo (publicación de las Naciones Unidas, núm. de venta S.17.XI.11), pág. 24.

en el 13º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, que la Asamblea General hizo suya en su resolución 70/174.

7. El Grupo de Expertos encargado de realizar un Estudio Exhaustivo sobre el Delito Cibernético ha celebrado un total de cuatro reuniones, en 2011, 2013, 2017 y 2018, respectivamente. En su resolución 22/7, de 26 de abril de 2013, la Comisión de Prevención del Delito y Justicia Penal tomó nota del estudio exhaustivo sobre el delito cibernético preparado por la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) bajo los auspicios del Grupo de Expertos y de las deliberaciones celebradas sobre su contenido en la segunda reunión del Grupo de Expertos, celebrada en Viena del 25 al 28 de febrero de 2013 (véase UNODC/CCPCJ/EG.4/2017/3) en la que se habían expresado diversos puntos de vista sobre el contenido, las conclusiones y las opciones que se presentaban en el estudio, y solicitó al Grupo de Expertos que, con la asistencia de la Secretaría, según procediera, prosiguiera su labor encaminada a cumplir su mandato.

8. En su resolución 26/4, aprobada en su 26º período de sesiones, el 26 de mayo de 2017, la Comisión de Prevención del Delito y Justicia Penal solicitó al Grupo de Expertos que prosiguiera su labor y, para ello, celebrara reuniones periódicas y funcionase como plataforma para impulsar el debate sobre cuestiones sustantivas relacionadas con el delito cibernético, siguiendo la evolución de las tendencias al respecto, y en consonancia con las Declaraciones de Salvador y Doha, y también solicitó al Grupo de Expertos que siguiera intercambiando información sobre legislación nacional, mejores prácticas, asistencia técnica y cooperación internacional, con miras a examinar opciones para fortalecer las actuales respuestas y proponer nuevas respuestas jurídicas o de otra índole frente al delito cibernético a nivel nacional e internacional. En esa misma resolución, la Comisión decidió que el Grupo de Expertos dedicase sus reuniones futuras a examinar de manera estructurada cada una de las cuestiones principales que se abordaban en el estudio, sin perjuicio de otros asuntos comprendidos en el mandato del Grupo de Expertos, teniendo en cuenta, según procediera, las contribuciones recibidas en cumplimiento de la resolución 22/7 de la Comisión y las deliberaciones de las reuniones anteriores del Grupo de Expertos.

9. En un contexto más amplio, cada vez se reconoce más, como se refleja en la Agenda 2030 para el Desarrollo Sostenible, aprobada por la Asamblea General en su resolución 70/1, que reducir los conflictos, la delincuencia, la violencia y la discriminación, y garantizar la inclusión, la buena gobernanza y el estado de derecho son esenciales para asegurar el desarrollo sostenible. El Objetivo 16 de la Agenda 2030 (“Promover sociedades pacíficas e inclusivas para el desarrollo sostenible, facilitar el acceso a la justicia para todos y construir a todos los niveles instituciones eficaces e inclusivas que rindan cuentas”) resulta particularmente pertinente en ese sentido. El Objetivo 16 está relacionado con la lucha contra la ciberdelincuencia que, junto con otras formas de delincuencia, incluida la delincuencia organizada, socava la buena gobernanza y el estado de derecho, pone en peligro la seguridad y el desarrollo, y tiene un efecto desestabilizador en los Estados Miembros (véase E/CN.7/2016/CRP.1-E/CN.15/2016/CRP.1, párr. 4).

10. En el 14º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, que se celebrará en el Japón en abril de 2020, se abordarán distintos aspectos de la ciberdelincuencia, entre otras cuestiones, en el contexto del cuarto curso práctico del Congreso en el que se tratará el tema “Tendencias delictivas actuales, fenómenos recientes y soluciones emergentes, en particular la utilización de las nuevas tecnologías como medio e instrumento contra el delito”.

11. En ese contexto, el debate temático sobre la ciberdelincuencia que se celebrará en el 27º período de sesiones de la Comisión tiene por objeto hacer un balance de los acontecimientos recientes. El debate temático servirá de plataforma para el debate ulterior y el intercambio de opiniones y experiencias entre los Estados Miembros. Para facilitar el debate temático, se han determinado ocho esferas temáticas relacionadas con la ciberdelincuencia, en particular esferas que están explícitamente incluidas en el tema principal. Cada una de esas ocho esferas temáticas se examina por separado en la

sección III más adelante, con diferentes acápites para las dificultades actuales y posibles respuestas (como se acordó en la continuación del 26º período de sesiones de la Comisión, véase el párr. 2 más arriba) y una lista indicativa de cuestiones o temas para su ulterior examen.

III. Esferas temáticas: temas de debate

A. Tipos de delitos cibernéticos y amenazas conexas

Dificultades actuales

12. El término “ciberdelincuencia” no es de índole jurídica ni forense; tampoco define ni describe una categoría claramente establecida de delito. Hay acuerdo general en torno a una lista básica de tipos de abusos y delitos relacionados específicamente con las computadoras, pero más allá de tal acuerdo no hay aún un consenso mundial sobre el significado del término. Esta situación es el resultado del carácter omnipresente de las computadoras y su versatilidad, así como de la evolución dinámica de las TIC y las formas en que se han venido utilizando desde fines del decenio de 1950.

13. Según el contexto, el término “ciberdelincuencia” puede referirse o bien a delitos cometidos por medio de las TIC, a delitos cometidos contra las instalaciones de las TIC y sus usuarios o bien a supuestos delictivos en los que las TIC desempeñan un papel indirecto o de apoyo[2]. Se ha utilizado el término “ciberdelincuencia” para describir una amplia variedad de delitos, incluidos los delitos contra los datos y sistemas informáticos (como la piratería informática), la falsificación y el fraude informáticos (como el *phishing*), los delitos de contenido (como la difusión de material relacionado con los abusos sexuales contra los niños)[3] y los delitos de derechos de autor (como la difusión de contenido pirateado).

14. La utilización cada vez mayor de la tecnología informática y la tendencia hacia la digitalización de los datos han aumentado la importancia de los datos informáticos. Como consecuencia de ello, los datos informáticos han pasado a ser blanco de ataques frecuentes que abarcan desde la interferencia de datos hasta el espionaje de datos. En la actualidad existe una economía sumergida digital compleja en la que los datos son el producto básico. Tienen valor monetario los datos personales y financieros robados que se utilizan, por ejemplo, para obtener acceso a cuentas bancarias y tarjetas de crédito existentes o para establecer nuevas líneas de crédito de manera fraudulenta. Esta situación da lugar a una serie de actividades delictivas, en particular el *phishing*, el *pharming*, la distribución de programas maliciosos y la piratería de bases de datos de empresas, que cuentan con el apoyo de una vasta infraestructura de autores de códigos de programas maliciosos, sitios especializados que acogen páginas web y personas que son capaces de arrendar redes de computadoras afectadas para llevar a cabo ataques automatizados.

15. El desarrollo y la distribución de programas maliciosos, en particular, siguen siendo la piedra angular de la mayoría de los casos de ciberdelincuencia. Desde fines de 2013, los criptoprogramas informáticos (programas maliciosos secuestradores que utilizan cifrado) han pasado a ser los principales programas maliciosos en función de la amenaza y las consecuencias que suponen. Siguiendo la tendencia de los ladrones de información, las campañas de criptoprogramas informáticos se dirigen cada vez más contra entidades de los sectores público y privado[4].

---

[2] Christopher Ram, “Cybercrime”, en *Routledge Handbook of Transnational Criminal Law*, Neil Boister y Robert J. Currie, coords. (Nueva York, Routledge, 2015), pág. 379.

[3] Véase el estudio de los efectos de la nueva tecnología de la información en los abusos y explotación de los niños, preparado por la Oficina de las Naciones Unidas contra la Droga y el Delito (Viena, 2015).

[4] Oficina Europea de Policía, *European Union Serious and Organised Crime Threat Assessment: Crime in the Age of Technology* (La Haya, 2017), pág. 30.

16. Los delincuentes procuran continuamente hallar métodos y tecnologías que les permitan hacer más eficaces sus modalidades de operación e incrementar sus márgenes de beneficio. El carácter anónimo de las transacciones en línea y el uso de las criptomonedas reducen el riesgo de detección por parte de las autoridades encargadas de hacer cumplir la ley. El mayor uso de las redes privadas virtuales, los *onion routers* o sistemas de encaminamiento cebolla y la traducción de direcciones de red de nivel operador (donde varios clientes comparten las direcciones de los protocolos Internet) limita la capacidad de los investigadores de atribuir las pruebas.

17. Las tasas de ciberdelincuencia siguen aumentando con la expansión de Internet, lo que está elevando a nuevos niveles la vulnerabilidad de los usuarios de Internet. Además, la amenaza que representa la ciberdelincuencia en sus diversas formas es multidimensional y está dirigida no solo contra los ciudadanos, sino también cada vez más contra las empresas y los gobiernos. Los instrumentos de la ciberdelincuencia plantean una amenaza directa para la seguridad y desempeñan una función cada vez más importante en la facilitación de la mayoría de las formas de delincuencia organizada y terrorismo.

Posibles respuestas

18. La escala sin precedentes del problema, junto con los múltiples tipos de conducta que se definen como delito cibernético, amenazan la capacidad de las autoridades para responder de manera efectiva y eficaz. Al mismo tiempo, el ciberespacio puede ofrecer también oportunidades e instrumentos para la detección del delito cibernético. El uso de las TIC por los delincuentes puede generar una serie de pistas de investigación y pruebas para el sistema de justicia penal. Las autoridades cuentan ahora con más datos que nunca sobre la actividad delictiva y tienen la oportunidad de aprovechar esa información de forma tal que la reunión de datos de inteligencia y la investigación resulten eficaces en función del costo. La explotación delictiva de las criptomonedas ofrece al respecto un ejemplo interesante. Las criptomonedas existen gracias a la tecnología de cadenas de bloques. A pesar de las lagunas técnicas y jurídicas existentes, varios aspectos de la tecnología de cadenas de bloques podrían convertir esa tecnología en un instrumento útil de aplicación de la ley para hallar pautas de transacciones sospechosas y rastrear pruebas (véase E/CN.15/2018/CRP.1, párr. 164).

19. Los investigadores informáticos cualificados que han recibido formación en el marco de actividades reforzadas de creación de capacidad pueden obtener pruebas electrónicas de los delitos cibernéticos, incluso cuando los autores hayan evitado cuidadosamente dejar huellas digitales o las hayan borrado. Dependiendo de los períodos de conservación de los datos, se pueden consultar los registros de conexión al protocolo Internet para establecer la hora y fecha, las fuentes y los destinos de las conexiones de Internet.

20. Además, el hecho de que la sociedad dependa cada vez más de Internet y de la comunicación asistida por computadora ha llevado a las fuerzas del orden a elaborar instrumentos para investigar los delitos en línea o a utilizar, por ejemplo, los programas informáticos para descubrir pautas delictivas. Los organismos encargados de hacer cumplir la ley también utilizan los instrumentos de los medios sociales para mejorar sus relaciones con las comunidades locales y solicitar la cooperación del público en las investigaciones penales.

21. Por consiguiente, es esencial que los Estados consideren la posibilidad de elaborar estrategias multidisciplinarias para hacer frente a los desafíos y mejorar su capacidad para investigar y procesar con eficacia los casos que entrañen delitos cibernéticos. Las estrategias multidisciplinarias pueden abarcar desde medidas reglamentarias e iniciativas de formulación de políticas hasta programas de prevención de la ciberdelincuencia y formación de las autoridades competentes, como se examina a continuación.

Cuestiones para el debate

22. La Comisión tal vez desee considerar las siguientes cuestiones para someterlas a un debate ulterior:

a) ¿Qué enseñanzas se han extraído del análisis de la evolución de las pautas de la ciberdelincuencia?

b) ¿Cuál es la mejor manera de utilizar esas enseñanzas en la formulación de medidas reglamentarias y estrategias normativas eficaces para combatir la ciberdelincuencia en el plano nacional?

c) ¿Qué impacto tienen los diversos tipos de ciberdelincuencia en la capacidad de los Estados Miembros para llevar registros sistemáticos de los delitos conexos e intercambiar información con fines de aplicación de la ley en los planos regional e internacional, incluida la información sobre la participación de grupos delictivos organizados, los modus operandi utilizados por esos grupos y las técnicas utilizadas para detectar las distintas formas de ciberdelincuencia?

d) ¿En qué medida pueden aplicarse al ciberespacio las definiciones que figuran en la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional de las expresiones “grupo delictivo organizado” y “grupo estructurado”, incluso en los casos en que los delincuentes, a menudo protegidos por el anonimato, interactúan entre ellos sin saber quién es su interlocutor?

B. Medidas jurídicas para combatir la ciberdelincuencia: aspectos relacionados con la penalización

Dificultades actuales

23. Al evaluar las dificultades actuales con que se tropieza al elaborar respuestas jurídicas ante la ciberdelincuencia, conviene tener presente la manera en que esas dificultades surgieron y luego se multiplicaron a lo largo de los años. Históricamente, los servicios informáticos y las tecnologías relacionadas con Internet dieron lugar a nuevas formas de delincuencia poco después de su creación. Un ejemplo de ello es la creación de redes informáticas en el decenio de 1970 y el primer caso de acceso no autorizado a esas redes, que se produjo muy poco después. Asimismo, los primeros delitos informáticos se perpetraron poco después de la introducción de las computadoras personales en el decenio de 1980, cuando se utilizaron computadoras personales para copiar productos de software. A fines del decenio de 1990, las redes habían pasado a ser una parte fundamental de la infraestructura de las TIC, lo que dio lugar a mayores preocupaciones en cuanto a determinadas formas de ciberdelincuencia que representaban una amenaza para las redes. Ello a su vez dio lugar a la utilización de la ciberseguridad y a una tendencia a tipificar específicamente como delito determinados tipos de ataques contra infraestructuras esenciales o a imponer penas más severas en esos casos[5].

24. Aparte de la aparición de nuevas definiciones y conceptos basados en la rápida evolución de la tecnología, persiste la cuestión de si debe tratarse la ciberdelincuencia como un fenómeno nuevo y tipificar delitos totalmente nuevos en relación con ella o si se debe intentar aplicar las definiciones existentes de los delitos y, en caso necesario, ampliarlas o adaptarlas. Algunos países han promulgado nuevas leyes en las que se tipifica el fraude informático como un delito específico, mientras que otros han tipificado como delitos nuevos la copia ilícita de datos o el daño a los datos, la obstaculización del acceso a los datos o el uso indebido de datos, debido a que las

[5] Véase, entre otros, Aunshul Rege-Patwardhan, “Cybercrimes against critical infrastructures: a study of online criminal organization and techniques”, *Criminal Justice Studies: A Critical Journal of Crime, Law and Society*, vol. 22, núm. 3 (2009), pág. 261; Luca Montanari y Leonardo Querzoni, coords., *Critical Infrastructure Protection: Threats, Attacks and Countermeasures* (marzo de 2014). Véase también la resolución 2341 (2017) del Consejo de Seguridad relativa a las amenazas a la paz y la seguridad internacionales causadas por actos terroristas.

definiciones existentes se referían únicamente a los bienes corporales. Otro ejemplo es la tipificación del robo de identidad como delito específico en algunas jurisdicciones.

25. En los casos en los que se opta por introducir ajustes en la legislación penal ya existente, los órganos legislativos se enfrentan a menudo a largos procedimientos para revisar y actualizar la ley. Por lo tanto, la principal dificultad estriba en el plazo de tiempo que transcurre entre el descubrimiento de nuevas formas de abuso delictivo y la promulgación de las modificaciones legislativas necesarias para hacerles frente. Ese desafío mantiene su importancia y vigencia a medida que se acelera la innovación de las TIC.

Posibles respuestas

26. Una legislación penal apropiada constituye la base de la investigación y el enjuiciamiento de los delitos cibernéticos. Por consiguiente, los legisladores deberán estar en condiciones de responder a la evolución de las TIC y vigilar de forma continua la eficacia de las disposiciones jurídicas existentes. Es necesario un análisis exhaustivo de la legislación vigente para determinar la existencia de posibles lagunas y hacer frente a las dificultades que plantea cumplir el requisito de la doble incriminación en el contexto de la cooperación internacional. Los legisladores también podrían beneficiarse de instrumentos multilaterales de carácter vinculante y no vinculante.

27. Para que tengan un efecto duradero, tal vez sea necesario que las nuevas leyes y las modificaciones de las leyes vigentes se redacten de forma flexible y tecnológicamente neutral, teniendo en cuenta la necesidad de seguridad y precisión jurídicas. La legislación también deberá atender la necesidad del acceso oportuno a la información a través de las fronteras nacionales. Por último, los legisladores tal vez requieran formación y orientación para formular disposiciones sólidas y promulgar leyes eficaces.

Cuestiones para el debate

28. La Comisión tal vez desee considerar las siguientes cuestiones para someterlas a un debate ulterior:

a) ¿Qué enseñanzas se han extraído de las iniciativas a nivel nacional para elaborar y aplicar leyes contra la ciberdelincuencia e integrar esa legislación en el marco más amplio de una estrategia nacional sobre la ciberdelincuencia?

b) ¿Ofrecen las leyes nacionales una base jurídica suficiente para la detección, investigación y enjuiciamiento eficaces de todos los delitos relacionados con la ciberdelincuencia? ¿Cuáles son las deficiencias que deben abordarse?

c) ¿Qué impacto tienen los instrumentos multilaterales existentes en el alcance de los marcos jurídicos nacionales de lucha contra la ciberdelincuencia? ¿Se ha logrado la convergencia de las respuestas jurídicas nacionales basadas en esos instrumentos y, de ser así, en qué medida?

d) Teniendo en cuenta el requisito de la doble incriminación, ¿influye la diversidad de enfoques nacionales en materia de penalización de los delitos cibernéticos en el alcance de la cooperación internacional?

C. Competencias procesales y pruebas electrónicas

Dificultades actuales

29. Las competencias de investigación nacionales desempeñan un papel fundamental en la reunión de pruebas electrónicas. El examen de las competencias de investigación en el plano nacional revela una diversidad considerable de enfoques sobre la utilización de pruebas electrónicas en la investigación de delitos. Esos enfoques se refieren a la medida en que puede interpretarse que las competencias preexistentes se aplican a los datos como pruebas intangibles y a la autoridad jurídica que existe para la adopción de medidas especialmente invasivas, como las investigaciones forenses a distancia. Si bien

las competencias jurídicas varían, debería disponerse de un conjunto de medidas de investigación específicas para la reunión de pruebas electrónicas. Esas medidas pueden incluir la conservación rápida de datos informáticos; las órdenes de acceso a datos de contenido almacenados; las órdenes de acceso a datos de tráfico almacenados; las órdenes de acceso a la información sobre los abonados; la obtención en tiempo real de datos de contenido; la obtención en tiempo real de datos de tráfico; la búsqueda de equipo o datos informáticos; la incautación de equipo o datos informáticos; el acceso transfronterizo a un sistema informático o datos informáticos; y la utilización de instrumentos de análisis forense a distancia. En el archivo de datos sobre ciberdelincuencia de la UNODC y el portal de gestión de conocimientos para el intercambio de recursos electrónicos y legislación sobre delincuencia (SHERLOC) se pueden encontrar ejemplos de leyes nacionales sobre medidas de investigación. Las competencias de investigación deben seguir el ritmo de la tecnología moderna. También deben contar con el respaldo de marcos jurídicos e institucionales que faciliten la coordinación y cooperación oportunas y eficaces entre el sector privado y los organismos gubernamentales competentes en los planos nacional, regional e internacional, y respetar al mismo tiempo los derechos humanos. Es fundamental que esos marcos tengan un fuerte componente de derechos humanos, puesto que las tecnologías de la información y de las comunicaciones afectan esferas como la privacidad y la libertad de expresión.

30. Lo ideal es que las pruebas electrónicas sean admisibles ante los tribunales. Sin embargo, la importancia cada vez mayor de las pruebas electrónicas en los procesos penales plantea dificultades que anteriormente se desconocían. Por ejemplo, las pruebas electrónicas son sumamente frágiles y pueden modificarse o borrarse con facilidad. En consecuencia, uno de los principales pasos en la informática forense es salvaguardar la integridad de las pruebas electrónicas. La protección de la integridad de los datos también es necesaria para garantizar la fiabilidad y la precisión de las pruebas. Además, para ser admisibles, las pruebas electrónicas deben reunirse mediante procedimientos establecidos para salvaguardar los derechos humanos.

31. Además, a fin de que las autoridades encargadas de hacer cumplir la ley investiguen eficazmente y reúnan pruebas electrónicas relacionadas con la ciberdelincuencia, la cooperación con otros agentes pertinentes, incluido el sector privado, ha adquirido especial importancia en los últimos años. En general, los proveedores de servicios de comunicaciones desempeñan una importante función en lo que respecta a la accesibilidad de las pruebas electrónicas. Las leyes nacionales sobre privacidad pueden afectar la capacidad de los proveedores para intercambiar información con las autoridades en el marco de una investigación.

Posibles respuestas

32. Debido a que las pruebas electrónicas son inestables, hay determinadas normas y requisitos necesarios para utilizar esas pruebas y garantizar su autenticidad e integridad. Esas normas y requisitos incluyen normas y procedimientos generales, como el mantenimiento de expedientes de los casos, el uso de tecnologías ampliamente aceptadas y la participación de expertos cualificados en las investigaciones.

33. Un número cada vez mayor de investigaciones sobre delitos cibernéticos, en particular en los casos relacionados con el abuso y la explotación de niños, exigen pruebas electrónicas que se encuentran en poder de terceros. Por consiguiente, es fundamental que la industria y los gobiernos colaboren para crear mecanismos que den a las autoridades encargadas de hacer cumplir la ley acceso oportuno a los datos en situaciones de urgencia. Esos mecanismos deberían combinarse con procesos jurídicos justos y transparentes en cuyo marco se realicen las investigaciones de rutina.

34. Una reunión del grupo de expertos sobre el acceso legítimo transfronterizo a datos digitales, organizada conjuntamente por la UNODC y la Dirección Ejecutiva del Comité contra el Terrorismo, en cooperación con la Asociación Internacional de Fiscales, se celebró en Viena los días 12 y 13 de febrero de 2018. El objetivo de la reunión era sentar las bases para la elaboración de una guía práctica dirigida a autoridades centrales,

fiscales e investigadores para la obtención de pruebas electrónicas de jurisdicciones extranjeras en investigaciones transfronterizas de lucha contra el terrorismo y la delincuencia organizada conexa. La reunión ofreció a los participantes la oportunidad de intercambiar leyes y guías nacionales, así como ejemplos de casos reales que demostraban buenas prácticas y enseñanzas extraídas a partir de la obtención de pruebas electrónicas de los proveedores de servicios de comunicaciones ubicados en jurisdicciones extranjeras.

Cuestiones para el debate

35. La Comisión tal vez desee considerar las siguientes cuestiones para someterlas a un debate ulterior:

a) ¿Con qué dificultades tropiezan las autoridades investigadoras cuando intentan cumplir los requisitos para utilizar las técnicas especiales de investigación y de reunión e intercambio de pruebas electrónicas para detectar, investigar y enjuiciar los delitos cibernéticos, y qué buenas prácticas sirven para responder a esas dificultades?

b) ¿Cuál ha sido la experiencia acumulada en los Estados Miembros en lo que respecta a la admisibilidad de esas pruebas en los tribunales?

c) ¿Qué impacto tiene la colaboración con el sector financiero en la recopilación de pruebas electrónicas relativas al producto del delito cibernético (por ejemplo, los traficantes de dinero)?

d) Desde una perspectiva del estado de derecho y los derechos humanos, ¿cuáles son las dificultades principales para la utilización y aplicación eficaces de técnicas relacionadas con la investigación y el enjuiciamiento del delito cibernético?

e) ¿Qué enseñanzas se han extraído de las iniciativas encaminadas a fomentar la cooperación entre las autoridades encargadas de hacer cumplir la ley y los proveedores de servicios de comunicaciones a fin de obtener pruebas electrónicas para la detección, investigación y enjuiciamiento del delito cibernético?

D. Cuestiones jurisdiccionales

Dificultades actuales

36. En el derecho internacional se prevé una serie de bases para el establecimiento de jurisdicción sobre actos de ciberdelincuencia, principalmente formas de jurisdicción basadas en el territorio y la nacionalidad. Pueden hallarse algunas de esas bases en los instrumentos sobre ciberdelincuencia multilaterales. En la actualidad, la jurisdicción territorial ampliada u objetiva suele basarse en la existencia de un elemento constitutivo del delito o sus efectos en el territorio de un Estado o de algún otro vínculo importante con el territorio de un Estado. Los Estados también deben determinar qué país está en la mejor situación para enjuiciar a los presuntos delincuentes basándose en factores como la ubicación de las pruebas o el lugar en que se encuentren los delincuentes.

37. La aplicación de una gama de bases jurisdiccionales por parte de diferentes países puede dar lugar a que más de un país establezca su jurisdicción sobre el mismo acto de ciberdelincuencia. El riesgo de conflictos jurisdiccionales aumenta aún más si se aplica el principio de territorialidad a casos en los que solo la infraestructura utilizada para la comisión de un delito se encuentra en el país de que se trata, no así el autor ni la víctima del delito.

38. La computación en la nube plantea una serie de dificultades para la justicia penal, en particular en lo que respecta a la ley aplicable y a la jurisdicción penal de ejecución. A menudo no resulta claro para las autoridades de justicia penal en qué jurisdicción están almacenados los datos ni cuál es el régimen jurídico que se les aplica. Un proveedor de servicios puede tener su sede en un país pero puede estar sujeto al régimen jurídico de un segundo país y los datos pueden estar almacenados en un tercer país. Los mismos datos pueden almacenarse en varios países utilizando la técnica de *mirroring* o

duplicación, o pueden transferirse de una jurisdicción a otra, lo cual complica aún más estos problemas.

39. Además, a menudo no está claro si un proveedor de servicios de computación en la nube es el agente que controla o el que procesa los datos que pertenecen a un usuario y, por lo tanto, no resulta claro qué normas se aplican. Otro factor de incertidumbre estriba en si los datos están almacenados o si se encuentran en tránsito y, por consiguiente, si deben emitirse órdenes de presentación, órdenes de registro e incautación, órdenes de interceptación u órdenes de obtención en tiempo real y sobre qué base jurisdiccional. Además, el carácter no localizado de la computación en la nube ocasiona problemas para la investigación forense y los registros en línea debido a la estructura de la nube (capacidad multiusuario, distribución y segregación de datos), y debido a los problemas jurídicos relacionados con la integridad y validez de la recopilación de datos, el control de las pruebas, la propiedad de los datos o la jurisdicción[6].

Posibles respuestas

40. En muchos casos, varios Estados pueden reclamar la jurisdicción sobre los delitos cibernéticos y es importante llevar a cabo consultas para decidir en qué Estado deberá celebrarse el juicio. Esa decisión puede entrañar cuestiones jurídicas, diplomáticas y prácticas, como las reclamaciones de jurisdicción y otras reclamaciones jurídicas formuladas por cada Estado, la cuestión de si los delincuentes pueden ser extraditados al Estado que desea enjuiciarlos, y consideraciones pragmáticas como el costo y otros obstáculos que impidan transferir las pruebas de un Estado a otro, la cuestión de garantizar que las pruebas se admitan en los tribunales y la presentación efectiva de las pruebas ante el tribunal. Cuando surgen conflictos jurisdiccionales, generalmente se resuelven mediante consultas oficiales u oficiosas entre los países. En los casos en que se decide que uno de varios Estados posibles debe incoar la acción judicial, puede transferirse efectivamente la jurisdicción de otros Estados. La remisión de actuaciones penales, como forma especial de cooperación internacional, proporciona el contexto y el marco para hacerlo[7].

41. Se ha llevado a cabo una labor a nivel multilateral a fin de reforzar la cooperación en los planos internacional y regional para obtener pruebas electrónicas. En junio de 2017, el Comité del Convenio sobre la Ciberdelincuencia del Consejo de Europa aprobó la preparación de un segundo protocolo del Convenio sobre la Ciberdelincuencia encaminado a establecer normas claras y procedimientos más eficaces para obtener pruebas electrónicas “en la nube” en investigaciones penales concretas. El mandato se aprobó el 8 de junio de 2017 y está previsto que las negociaciones se celebren entre septiembre de 2017 y diciembre de 2019.

Cuestiones para el debate

42. La Comisión tal vez desee considerar las siguientes cuestiones para someterlas a un debate ulterior:

a) ¿Cuáles son los criterios por los que se rige la jurisdicción a los efectos de ejecutar las respuestas de la justicia penal en casos de delito cibernético? ¿Cómo se aplican esos criterios a situaciones de computación en la nube en las que los datos no suelen estar “en reposo”?

[6] Consejo de Europa, Comité del Convenio sobre la Ciberdelincuencia (T-CY), “Criminal justice access to data in the cloud: challenges”, documento de debate preparado por el Grupo sobre pruebas en la nube, 26 de mayo de 2015, documento T-CY (2015)10, págs. 10 a 14.

[7] Véase el documento de antecedentes preparado por la Secretaría sobre las consideraciones prácticas, las buenas prácticas y las dificultades encontradas en el ámbito de la remisión de las actuaciones penales como forma diferenciada de cooperación internacional en asuntos penales (CTOC/COP/WG.3/2017/2).

b) ¿Cuál ha sido la experiencia acumulada en la celebración de consultas para resolver conflictos de jurisdicción sobre delitos cibernéticos? ¿Cuáles son las dificultades, cuáles son las buenas prácticas y qué enseñanzas se han extraído?

E. Coordinación y cooperación entre organismos en el plano nacional

Dificultades actuales

43. Las estrategias de interesados múltiples sobre ciberdelincuencia son un elemento fundamental en la lucha contra este tipo de delito. Los desafíos jurídicos, técnicos e institucionales que plantea la ciberdelincuencia son de gran alcance y solo pueden abordarse si se sigue una estrategia coherente basada en las iniciativas existentes y en la función de los distintos interesados. Para ser eficaz, la lucha contra la ciberdelincuencia requiere estructuras organizativas muy desarrolladas que eviten la superposición y tengan competencias claramente definidas y puedan coordinar a todas las partes interesadas a fin de adoptar medidas concertadas. Sin las estructuras adecuadas, será sumamente difícil aplicar políticas sólidas e iniciativas programáticas.

44. La disuasión de la ciberdelincuencia es también un componente integral de las estrategias nacionales para garantizar la ciberseguridad y proteger las infraestructuras de información esenciales. Ello incluye, en particular, la aprobación de leyes para luchar contra el uso indebido de las TIC con fines delictivos y de otra índole y combatir las actividades dirigidas a comprometer la integridad de las infraestructuras nacionales esenciales. La disuasión de la ciberdelincuencia es una responsabilidad que comparten las autoridades gubernamentales, el sector privado y los ciudadanos y que requiere la adopción de medidas coordinadas de prevención, preparación, respuesta y recuperación ante incidentes de ciberseguridad. La formulación y aplicación de una estrategia nacional de lucha contra la ciberdelincuencia requiere un enfoque amplio que entrañe la colaboración y coordinación entre los interesados pertinentes a nivel institucional.

45. Sin embargo, la coordinación institucional plantea una serie de dificultades, la mayoría de las cuales se relacionan con los recursos y la capacidad que cada país tiene a su disposición. Deben tenerse en cuenta varios otros factores, incluido el grado de apoyo del sector privado, por ejemplo mediante alianzas público-privadas, o las medidas de autorregulación y de autoprotección vigentes en el sector privado.

Posibles respuestas

46. El establecimiento de alianzas interinstitucionales se ha convertido en una práctica común, a nivel estratégico, para combatir la ciberdelincuencia, incluidos los delitos contra los niños, facilitados por la tecnología. En respuesta a las dificultades múltiples con que se tropieza en la lucha contra la ciberdelincuencia, los proveedores de servicios de comunicaciones y las instituciones públicas, como las autoridades policiales y de justicia penal, tienen que crear alianzas público-privadas en las que se fomente la confianza y los diálogos bilaterales. En términos más generales, los Estados deben organizar respuestas normativas que vayan más allá del derecho penal y ofrecer incentivos al sector privado para que participe activamente en la prevención del delito. Tal enfoque puede ser útil para crear un entorno sensible a las nuevas amenazas que propicie la lucha contra esas amenazas.

47. Los equipos de tareas que actúan específicamente contra la delincuencia organizada facilitada por Internet podrían ser un instrumento útil para la adopción de medidas concertadas contra la ciberdelincuencia. Esos equipos de tareas deberán responder a la evolución del entorno delictivo y podrían dar lugar, por ejemplo, al establecimiento de grupos más permanentes para el intercambio de información y de más arreglos especiales para operaciones específicas, como la desarticulación de *botnets*. En todos los casos, las autoridades deben tener la flexibilidad necesaria para hacer participar a diversos interesados, como los organismos encargados de hacer cumplir la ley, el sector privado, el mundo académico y los grupos de usuarios, y para coordinar de manera eficiente con ellos a fin de lograr los resultados deseados.

48. Internet ha cambiado el enfoque de la regulación gubernamental de las TIC en los gobiernos. Las autoridades que regulan el sector de las TIC ya están participando en una serie de actividades para hacer frente al delito cibernético, en particular, en esferas como la regulación del contenido, la seguridad de la red y la protección del consumidor, puesto que los usuarios se han vuelto vulnerables. En consecuencia, la implicación de los organismos reguladores es el resultado del hecho de que el delito cibernético socava el desarrollo de la industria de las TIC y de las partes que ofrecen productos y servicios conexos. Las nuevas obligaciones y responsabilidades de los organismos reguladores de las TIC en la lucha contra la ciberdelincuencia puede considerarse parte de la tendencia más amplia hacia la conversión de los modelos centralizados de regulación en materia de ciberdelincuencia en estructuras flexibles[8].

Cuestiones para el debate

49. La Comisión tal vez desee considerar las siguientes cuestiones para someterlas a un debate ulterior:

a) ¿Con qué problemas se ha tropezado en el plano nacional en lo que respecta al fortalecimiento de la capacidad institucional y la coordinación interinstitucional para hacer frente al delito cibernético?

b) ¿Se ha acumulado alguna experiencia en la elaboración de marcos modelo o directrices para la cooperación entre los interesados pertinentes en el plano nacional para prevenir y combatir la ciberdelincuencia? En caso afirmativo, ¿de qué manera fomentaron esos marcos modelo o directrices la colaboración efectiva?

F. Cooperación internacional

Dificultades actuales

50. Además de tipificar como delito los actos de ciberdelincuencia y conferir competencias procesales conexas, los instrumentos existentes establecen mecanismos para la cooperación internacional en la investigación transfronteriza y el enjuiciamiento de los delitos cibernéticos. La cooperación internacional para combatir la ciberdelincuencia representa un creciente desafío para la justicia penal y las autoridades encargadas de hacer cumplir la ley. Si bien en teoría la ubicación de datos informáticos concretos puede determinarse en un momento dado, con la llegada de la computación en la nube, el cifrado y el intercambio y almacenamiento de datos entre homólogos, los datos ahora pueden existir en forma de ejemplares múltiples distribuidos en diferentes dispositivos y ubicaciones, y pueden trasladarse a otra ubicación geográfica en cuestión de segundos[9].

51. Debido al carácter inestable de las pruebas electrónicas, la cooperación internacional en asuntos de ciberdelincuencia requiere una respuesta oportuna, en particular la conservación y presentación de datos por parte de los proveedores de servicios, y la capacidad de solicitar medidas de investigación especializadas. Una de las dificultades con que se tropieza comúnmente al solicitar esos datos a otra jurisdicción son las demoras en la respuesta, que suelen superar el período de conservación de datos y permiten a los autores de delitos destruir pruebas electrónicas clave de manera permanente. Otras dificultades comunes son la falta de compromiso y flexibilidad por parte de la autoridad requerida, la cuestión de si esa autoridad

[8] Unión Internacional de Telecomunicaciones, *Understanding Cybercrime: Phenomena, Challenges and Legal Response* (Ginebra, 2012), pág. 101.

[9] Documento de antecedentes acerca del seminario 3, sobre el fortalecimiento de las respuestas de prevención del delito y justicia penal frente a las formas de delincuencia en evolución, como la ciberdelincuencia y el tráfico de bienes culturales, incluidas las lecciones aprendidas y la cooperación internacional (A/CONF.222/12), párr. 32.

proporciona las pruebas de forma tal que puedan utilizarse en los procesos penales y las diferencias en las definiciones de los delitos en los Estados que cooperan[10].

52. En la segunda reunión del Grupo de Expertos encargado de realizar un Estudio Exhaustivo sobre el Delito Cibernético, celebrada en 2013, la mayoría de los expertos se mostraron de acuerdo en que para luchar contra el problema del delito cibernético era necesario aumentar y acelerar la cooperación internacional, especialmente porque el problema seguía creciendo y la dependencia de las tecnologías para fines legítimos agravaba el potencial de amenaza del delito cibernético. Más allá de eso, se expresaron distintas opiniones sobre cuál era el mejor enfoque estratégico y las prioridades para hacer frente a los problemas derivados del delito cibernético[11]. En ese contexto, ha habido controversia sobre si debería crearse un nuevo instrumento jurídico universal de lucha contra la ciberdelincuencia para abordar, entre otras cosas, aspectos de la cooperación internacional a nivel mundial, o si, por el contrario, la comunidad internacional debería seguir dependiendo de los instrumentos multilaterales existentes, como el Convenio del Consejo de Europa sobre la Ciberdelincuencia. La cuestión sigue siendo objeto de debate, sin que se haya llegado a un consenso hasta la fecha.

Posibles respuestas

53. Se podrían mejorar aún más los mecanismos de cooperación internacional examinando la manera de agilizar los procesos de asistencia judicial recíproca. Otras soluciones pueden estribar en el fortalecimiento de la cooperación en la aplicación de la ley y la reanudación del diálogo multilateral sobre el acceso transnacional a los datos informáticos. Por ejemplo, el establecimiento de un régimen aparte para el acceso a la información sobre los abonados, según se define en el artículo 18, párrafo 3, del Convenio del Consejo de Europa sobre la Ciberdelincuencia, y la diferenciación entre los tipos de datos buscados podrían contribuir en gran medida a una mayor eficiencia de la asistencia judicial recíproca en el ámbito de la ciberdelincuencia y las pruebas electrónicas[12].

54. Las innovaciones como la inclusión de un módulo sobre pruebas electrónicas en el nuevo programa para redactar solicitudes de asistencia judicial recíproca de la UNODC pueden ayudar a racionalizar los procesos de asistencia judicial recíproca que entrañan pruebas electrónicas. Al mismo tiempo, sin embargo, cada vez podría ser más necesario que los encargados de hacer cumplir la ley encuentren formas innovadoras de colaborar en las investigaciones transnacionales de delitos cibernéticos. La participación de entidades como el Complejo Mundial para la Innovación de la Organización Internacional de Policía Criminal (INTERPOL) y el Centro Europeo contra la Delincuencia Informática de la Oficina Europea de Policía (Europol) en la coordinación y apoyo de las investigaciones transnacionales, incluso facilitando el intercambio de información entre las autoridades encargadas de hacer cumplir la ley, puede resultar especialmente importante en ese sentido.

55. Entre otras soluciones cabe citar las siguientes: establecer en las autoridades centrales unidades separadas para investigar los delitos cibernéticos; vigilar y examinar las prácticas relativas a los casos en materia de asistencia judicial recíproca para analizar la capacidad de respuesta y la eficiencia, en particular llevando estadísticas de las solicitudes de asistencia judicial recíproca que entrañen pruebas electrónicas; utilizar más frecuentemente la cooperación entre fuerzas de policía como complemento útil de las modalidades de asistencia judicial recíproca para asegurar respuestas oportunas a las solicitudes urgentes de asistencia; ofrecer una capacitación más centrada e intensiva para mejorar la asistencia judicial recíproca, la cooperación entre fuerzas de policía y

[10] Véase el documento de antecedentes preparado por la Secretaría sobre la reunión y el intercambio de pruebas electrónicas (CTOC/COP/WG.3/2015/2), párr. 19.

[11] Resumen del Relator sobre las deliberaciones de la segunda reunión del Grupo de Expertos encargado de realizar un Estudio Exhaustivo sobre el Delito Cibernético, celebrada en Viena del 25 al 28 de febrero de 2013 (UNODC/CCPCJ/EG.4/2017/3), párr. 25.

[12] Véase Consejo de Europa, Comité del Convenio sobre la Ciberdelincuencia, Grupo sobre pruebas en la nube, “Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY”, documento T-CY (2016)5, pág. 13.

otras formas de cooperación internacional en materia de ciberdelincuencia y pruebas electrónicas; intensificar el intercambio de información y experiencia entre las redes de puntos de contacto que ofrecen acceso las 24 horas; y asignar recursos a nivel de las autoridades nacionales encargadas de dar cumplimiento a las solicitudes de asistencia judicial recíproca, y mejorar la coordinación entre estas autoridades y las autoridades centrales en aras de una respuesta oportuna.

Cuestiones para el debate

56. La Comisión tal vez desee considerar las siguientes cuestiones para someterlas a un debate ulterior:

a) ¿De qué manera pueden agilizarse los procedimientos de asistencia judicial recíproca en casos que entrañen delitos cibernéticos y pruebas electrónicas? ¿Cuáles son las mejores prácticas y en qué estriban las dificultades en lo que respecta a la cooperación entre fuerzas de policía para el traslado de pruebas electrónicas al extranjero?

b) ¿Qué ejemplos pueden proporcionar los Estados de la manera en que la intensificación del intercambio de información en los planos regional e internacional ha contribuido a aumentar su capacidad para detectar y evaluar los riesgos y responder a las solicitudes de manera eficaz y oportuna?

c) ¿De qué manera deben redactarse, transmitirse y tramitarse las solicitudes internacionales de conservación de pruebas electrónicas? ¿Cuál ha sido la experiencia acumulada en materia de cooperación entre los sectores público y privado a ese respecto?

G. Prevención de la ciberdelincuencia

Dificultades actuales

57. Los costos y la complejidad que suponen la investigación y el enjuiciamiento de los casos de ciberdelincuencia sugieren que los beneficios de las iniciativas conjuntas de prevención pueden ser sustanciales. Las alianzas público-privadas, en particular, son fundamentales para la prevención del delito cibernético. Los proveedores de servicios pueden contribuir a la prevención del delito cibernético de dos maneras: a) almacenando los datos de los usuarios a los que los funcionarios encargados de hacer cumplir la ley en posesión de una orden judicial pueden tener acceso para utilizarlos en la investigación de delitos cibernéticos; y b) filtrando activamente las comunicaciones y el contenido de Internet con miras a prevenir los actos delictivos cibernéticos antes de que se cometan. Si se analizan, sin embargo, estas dos medidas en el contexto de la libertad de expresión, las dos plantean numerosos problemas.

58. Al analizar el papel de los proveedores de servicios en la prevención del delito cibernético, tal vez sea necesario considerar sus limitaciones como entidades del sector privado. En primer lugar, las políticas de los proveedores son a menudo inestables y carecen de previsibilidad para los organismos encargados de hacer cumplir la ley y también para los clientes. Los proveedores de servicios pueden modificar sus políticas unilateralmente en cualquier momento y sin previo aviso a los organismos encargados de hacer cumplir la ley. Además, las políticas y prácticas de unos y otros proveedores difieren ampliamente y difieren también ampliamente las políticas y prácticas de los diferentes Estados Miembros. Un proveedor puede responder a numerosas solicitudes de un país pero a ninguna o a unas pocas de otro país, mientras que las prácticas de otro proveedor pueden ser exactamente opuestas[13].

59. En segundo lugar, las investigaciones policiales de delitos cibernéticos pueden verse afectadas por las salvaguardias de protección de datos que exigen que los datos personales se borren cuando ya no se requieran para los fines para los cuales se

[13] *Ibid*., “Criminal justice access to data in the cloud: Cooperation with 'foreign' service providers” (T-CY (2016)2), pág. 22.

reunieron. Por consiguiente, si bien las leyes de conservación de datos pueden representar un enfoque pragmático para garantizar que los proveedores de servicios de comunicaciones cumplan una función más importante en la prevención de la ciberdelincuencia mediante una mayor cooperación con los organismos encargados de hacer cumplir la ley, es importante que esas leyes se apliquen con las debidas salvaguardias de procedimiento y protección de la privacidad. Las normas y reglamentos sobre la protección de los datos deben tenerse en cuenta, entre otras cosas, el reglamento general de protección de datos de la Unión Europea[14].

60. El mundo académico tiene ante sí el gran reto de subsanar las numerosas deficiencias que existen y siguen surgiendo en el acervo de conocimientos sobre ciberdelincuencia, en particular sobre el abuso y la explotación sexuales de los niños en relación con las TIC. En función de la financiación sostenible, que en muchos países constituye un importante desafío, las instituciones académicas pueden cumplir diversas funciones en la prevención del delito cibernético, incluso impartiendo educación y capacitación a los profesionales, contribuyendo a la formulación de leyes y políticas y al desarrollo de normas técnicas y soluciones.

Posibles respuestas

61. Las buenas prácticas en materia de prevención del delito cibernético incluyen la promulgación de leyes, una dirección eficaz, el desarrollo de la capacidad en materia de justicia penal y aplicación de la ley, el desarrollo de una sólida base de conocimientos y la cooperación entre el gobierno, las comunidades, el sector privado y los Estados. Es de suma importancia prestar asistencia en la elaboración y perfeccionamiento de técnicas de prevención, intercambiar las enseñanzas extraídas y las mejores prácticas e intercambiar la información necesaria para elaborar técnicas de prevención y dotarlas de eficacia.

62. Las campañas e iniciativas de sensibilización y educación, incluidas las relativas a las nuevas amenazas y las dirigidas a destinatarios concretos, como los niños, se han destacado como un componente importante de las políticas de prevención de la ciberdelincuencia [15]. La iniciativa de Educación para la Justicia, componente fundamental del Programa Mundial de la UNODC para la Aplicación de la Declaración de Doha, incluye la elaboración y difusión de material para combatir la ciberdelincuencia dirigido a niños y jóvenes en los niveles de enseñanza primario, secundario y superior.

63. La sociedad civil puede desempeñar una función fundamental en lo que respecta a ayudar a los niños a comprender los riesgos en línea y enfrentarse a ellos, lo que tiene particular importancia en la prevención del abuso y la explotación de niños facilitados por las TIC. La educación y los métodos de prevención psicosociales se reconocen como elemento esencial para proteger a los niños contra el abuso y la explotación facilitados por las TIC. Las iniciativas educativas permiten que los niños, sus familias y las personas que los atienden comprendan y evalúen adecuadamente los riesgos vinculados a las TIC[16].

64. Existen varios modelos de alianzas público-privadas que fomentan la prevención de la ciberdelincuencia, como las establecidas entre las autoridades encargadas de hacer cumplir la ley y los proveedores de servicios de comunicaciones. Muchos modelos recurren al intercambio de información sobre la base de normas claras, de confianza, de composición restringida, del estímulo que suponen los beneficios mutuos y de la capacidad de respuesta. Además, seguirá creciendo la función que desempeña el sector privado en la detección y el bloqueo, entre otras cosas, del material en línea relacionado

[14] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE (*Diario Oficial de la Unión Europea*, L 119, 4 de mayo de 2016, págs. 1 a 88).

[15] Véase el estudio de los efectos de las nuevas tecnologías de la información, pág. 54.

[16] *Ibid*., pág. 54.

con el abuso sexual de los niños antes de que los clientes puedan acceder a ese material[17].

65. Un enfoque claro y con visión de futuro para los Gobiernos supone colaborar con quienes ejercerán influencia en el futuro entorno empresarial y operativo, a fin de que todos los interesados logren adelantarse a los cambios en las conductas delictivas y el uso indebido de la tecnología. En ese contexto, será importante seguir profundizando los conocimientos sobre el comportamiento del autor contemporáneo de delitos cibernéticos mediante el análisis de la información de inteligencia, las investigaciones criminológicas y las técnicas de elaboración de perfiles, a fin de emplear los recursos existentes de manera más eficaz e identificar de manera proactiva las características de las tecnologías de las comunicaciones futuras que determinarán su susceptibilidad a la explotación delictiva.

Cuestiones para el debate

66. La Comisión tal vez desee considerar las siguientes cuestiones para someterlas a un debate ulterior:

a) ¿Qué ejemplos pueden proporcionar los Estados de estrategias eficaces de prevención entre los interesados pertinentes que participan en la lucha contra la ciberdelincuencia? ¿Cómo se definen los resultados satisfactorios y cómo se miden?

b) ¿Cuál es la mejor manera en que las instituciones académicas, el sector privado y las organizaciones no gubernamentales pueden contribuir a la elaboración y el intercambio de conocimientos, leyes y políticas en la esfera de la ciberdelincuencia?

c) ¿Cuál es la experiencia acumulada por los Estados Miembros en lo que respecta al equilibrio entre la protección de los datos y la eficacia de las investigaciones sobre ciberdelincuencia?

H. Creación de capacidad y asistencia técnica

Dificultades actuales

67. Es fundamental crear capacidad a nivel de los organismos nacionales encargados de hacer cumplir la ley y los sistemas de justicia penal. Si bien la mayoría de los países han comenzado a establecer estructuras especializadas para la investigación de los delitos cibernéticos y los delitos que entrañan pruebas electrónicas, en muchos países esas estructuras carecen de financiación suficiente y se ven afectadas por la falta de capacidad. Debido a que las pruebas electrónicas son esenciales para la investigación de los delitos cibernéticos, las autoridades encargadas de hacer cumplir la ley tal vez deban hacer una clara distinción entre los investigadores de delitos cibernéticos y la capacidad digital de los laboratorios forenses y establecer claramente asimismo los respectivos flujos de trabajo. Tal vez los funcionarios de los servicios de represión de primera línea deban adquirir y utilizar de manera creciente competencias básicas como las que se emplean para producir una imagen de un dispositivo de almacenamiento electrónico que sea utilizable con fines de examen forense.

68. En general, es evidente que el desarrollo de la capacidad de los agentes de los servicios de represión y de justicia penal para combatir la ciberdelincuencia será un proceso continuo, puesto que las innovaciones técnicas y delictivas siguen avanzando a un ritmo acelerado.

Posibles respuestas

69. La asistencia técnica y la cooperación son importantes para permitir el intercambio de buenas prácticas de investigación y de experiencias, así como la difusión de nuevas técnicas. Los Estados Miembros tal vez deseen mejorar el intercambio de nuevos enfoques de la investigación del fraude financiero complejo basado en Internet, el

[17] Véase, por ejemplo, *The Netclean Report 2017*, que puede consultarse en la direccion siguiente: https://www.netclean.com/netclean-report-2017.

tráfico de drogas en línea o el uso de monedas virtuales para el blanqueo de dinero, lo que permitiría a las autoridades encargadas de hacer cumplir la ley de diversos países adquirir rápidamente las competencias necesarias para combatir las nuevas amenazas en el ámbito de la ciberdelincuencia.

70. Las estructuras o unidades especializadas en delitos cibernéticos de los organismos encargados de hacer cumplir la ley pueden contribuir a que los Estados concentren sus limitados recursos en un solo órgano a fin de desarrollar técnicas de investigación especializadas y reunir y analizar pruebas electrónicas adecuadas, incluso mediante la realización de exámenes forenses digitales. Al mismo tiempo, esas estructuras o unidades pueden impartir capacitación a los organismos locales encargados de hacer cumplir la ley, coordinar las respuestas nacionales ante la ciberdelincuencia, facilitar la cooperación entre los asociados que participan en las investigaciones y concentrarse en determinadas formas de ciberdelincuencia que puedan ser motivo de especial preocupación para un Estado.

71. De conformidad con la resolución 65/230 de la Asamblea General y las resoluciones 22/7 y 22/8 de la Comisión de Prevención del Delito y Justicia Penal, la UNODC, por conducto de su Programa Mundial contra el Delito Cibernético, tiene el mandato de ayudar a los Estados Miembros en su lucha contra la ciberdelincuencia, mediante la creación de capacidad y la asistencia técnica. En el marco de ese Programa, la UNODC presta asistencia técnica concreta para la creación de capacidad, la prevención y la sensibilización, la cooperación internacional y el análisis en relación con la ciberdelincuencia, principalmente en los países en desarrollo. También presta asistencia legislativa, previa solicitud y dentro de los límites de su mandato, a los Estados Miembros que la necesitan.

72. Por ejemplo, la UNODC ha elaborado un curso de formación de capacitadores sobre la investigación de las criptomonedas y ha venido impartiendo capacitación en materia de investigación de las criptomonedas en diversas regiones. El objetivo de la capacitación es mejorar la capacidad de los funcionarios encargados de hacer cumplir la ley, los analistas, los fiscales y los jueces en relación con las criptomonedas, la localización de bitcoines en una investigación financiera, la localización de recursos de información y la colaboración en materia de tramitación de casos en el plano internacional.

Cuestiones para el debate

73. La Comisión tal vez desee considerar las siguientes cuestiones para someterlas a un debate ulterior:

a) ¿Qué aspectos de las medidas y estrategias relacionadas con la ciberdelincuencia tienen un alto grado de prioridad en la esfera de la asistencia técnica y la creación de capacidad, en particular en vista de la evolución de la ciberdelincuencia y las amenazas nuevas y emergentes vinculadas a ella?

b) ¿Qué enseñanzas se han extraído a partir del intercambio de buenas prácticas de investigación y experiencia, así como de la difusión de nuevas técnicas como ejemplo de cooperación en materia de asistencia técnica?

c) ¿Cuál es la mejor manera de lograr sinergias y promover alianzas entre las organizaciones internacionales que prestan asistencia técnica en la esfera de la ciberdelincuencia a fin de garantizar servicios tangibles y sostenibles de creación de capacidad a los Estados Miembros que necesitan asistencia?

IV. Abordar las deficiencias actuales, el camino a seguir

74. Cada vez son mayores los esfuerzos que realiza la comunidad internacional para comprender mejor las amenazas de la ciberdelincuencia y responder ante ellas. No obstante, es preciso redoblar esfuerzos ya que todavía se enfrentan dificultades considerables en la elaboración y aplicación de respuestas amplias, coordinadas, sostenibles y eficaces ante la ciberdelincuencia.

75. La Comisión, al facilitar en su 27º período de sesiones el debate temático durante sus deliberaciones sobre el tema pertinente del programa, servirá de plataforma para el intercambio de información, mejores prácticas y enseñanzas extraídas, en la preparación de respuestas eficaces y en la promoción de los instrumentos o normas internacionales pertinentes de lucha contra la ciberdelincuencia.

76. Al examinar nuevas medidas para abordar los desafíos que plantea el delito cibernético y el camino a seguir para elaborar respuestas adecuadas, la Comisión tal vez desee centrar el debate en los ámbitos de los marcos jurídicos e institucionales nacionales vigentes que parecen acarrear los mayores riesgos, y en las esferas prioritarias en las que los Estados Miembros se enfrentan a los mayores desafíos.

77. La Comisión podría considerar la posibilidad de recomendar a los Estados Miembros que refuercen aún más sus iniciativas de creación de capacidad y sus marcos jurídicos, en particular al examinar las políticas y leyes nacionales y los marcos institucionales vigentes con el objetivo de definir la legislación, los marcos institucionales y las prácticas nuevas o modificadas que pudieran fortalecer su capacidad de enfrentar las amenazas de la ciberdelincuencia existentes o nuevas.

78. La Comisión podría determinar y priorizar las esferas de la asistencia técnica que la UNODC puede prestar en estrecha colaboración y coordinación con otros agentes pertinentes, sobre la base de los mandatos pertinentes, para brindar un mayor apoyo a los Estados Miembros en la aplicación de las políticas y las leyes nacionales y la capacidad institucional para hacer frente a los desafíos actuales y emergentes vinculados a la ciberdelincuencia.

79. Además, la Comisión tal vez desee invitar a la UNODC a que le preste asistencia en lo que respecta a mantener la comunicación con otros órganos intergubernamentales que se ocupan de la ciberdelincuencia y de las respuestas de la justicia penal para prevenir y combatir ese fenómeno, en particular la Conferencia de las Partes en la Convención contra la Delincuencia Organizada Transnacional y su Grupo de Trabajo sobre Cooperación Internacional, en el marco de sus respectivos mandatos y según proceda.