Naciones Unidas E/CN.15/2013/24

# Consejo Económico y Social

Distr. general
5 de marzo de 2013
Español
Original: inglés

**Comisión de Prevención del Delito y Justicia Penal**
**22° período de sesiones**
Viena, 22 a 26 de abril de 2013
Tema 7 del programa provisional*
**Tendencias de la delincuencia a nivel mundial y nuevas cuestiones y respuestas relativas a la prevención del delito y la justicia penal**

## Promoción de las actividades relativas a la lucha contra el delito cibernético, incluidos la asistencia técnica y el fomento de la capacidad

### Informe del Secretario General

*Resumen*

El presente informe se ha preparado en cumplimiento de la resolución 20/7 de la Comisión de Prevención del Delito y Justicia Penal, titulada "Promoción de las actividades relativas a la lucha contra el delito cibernético, incluidos la asistencia técnica y el fomento de la capacidad". Contiene un resumen de las actividades de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) en lo referente a la prestación de asistencia tanto técnica como en el ámbito del fomento de la capacidad a los Estados Miembros, al igual que una sinopsis de las actividades realizadas por la UNODC en apoyo del Grupo de expertos encargado de realizar un estudio exhaustivo del problema del delito cibernético y un resumen ejecutivo del proyecto de estudio sobre el delito cibernético.

* E/CN.15/2013/1.

V.13-80776 (S) 080413 080413

# I. Introducción

1. El presente informe se ha preparado en cumplimiento de la resolución 20/7 de la Comisión de Prevención del Delito y Justicia Penal, titulada “Promoción de las actividades relativas a la lucha contra el delito cibernético, incluidos la asistencia técnica y el fomento de la capacidad”.

2. En esa resolución, la Comisión solicitó a la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) que, en cooperación con los Estados Miembros, las organizaciones internacionales y regionales pertinentes y, según procediera, el sector privado, siguiera prestando a los Estados que lo solicitaran asistencia técnica y capacitación basadas en las necesidades nacionales, especialmente con respecto a la prevención, detección, investigación y enjuiciamiento del delito cibernético en todas sus formas, sin perjuicio de la labor y los resultados de las reuniones del Grupo de expertos encargado de realizar 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.

3. Además, la Comisión tomó nota de los resultados de la primera reunión del Grupo de expertos (véase E/CN.15/2011/19) y solicitó a la UNODC que reforzara la cooperación con los Estados Miembros, con organizaciones pertinentes como la Organización Internacional de Policía Criminal (INTERPOL), la Oficina Europea de Policía, la Unión Internacional de Telecomunicaciones (UIT), la Comisión Europea, el Consejo de Europa, la Organización de Cooperación de Shanghái y la Comunidad de Estados Independientes, así como con el sector privado, incluidas las empresas informáticas y los proveedores de servicios de Internet, a fin de combatir los delitos cibernéticos.

# II. Labor realizada por la Oficina de las Naciones Unidas contra la Droga y el Delito, en cooperación con los Estados Miembros, las organizaciones internacionales y regionales y el sector privado, con objeto de proporcionar asistencia técnica y capacitación a los Estados

4. En 2012 la UNODC ultimó el programa mundial contra el delito cibernético, en el que se adoptó un enfoque amplio centrado en los siguientes aspectos: a) actividades de capacitación para las fuerzas del orden y los profesionales de la justicia penal sobre las técnicas de investigación del delito cibernético y las formas de abordarlo desde la perspectiva de la justicia penal; b) prevención del delito cibernético y sensibilización a este fenómeno; c) mayor cooperación nacional, regional e internacional para hacer frente al delito cibernético; y d) reunión de datos, investigación y análisis de los vínculos entre la delincuencia organizada y el delito cibernético. En el marco de ese programa, la UNODC promoverá el fomento de la capacidad sostenible y a largo plazo, incluso mediante sesiones de capacitación, en cooperación con diferentes asociados, como la UIT, el sector privado y expertos académicos.

5. El objetivo de todas las actividades del programa mundial contra el delito cibernético es propiciar un aumento de la capacidad nacional sostenible a largo plazo para prevenir y combatir el delito cibernético. La realización de las actividades previstas en el programa estará a cargo principalmente de la UNODC, como organismo de ejecución, con el apoyo adicional de la UIT y otros asociados competentes, en caso necesario y según el asunto de que se trate, las solicitudes de los gobiernos y el mandato pertinente.

6. En mayo de 2011 la UNODC suscribió un memorando de entendimiento con la UIT a fin de favorecer la cooperación en la prestación de asistencia técnica en la esfera del delito cibernético y la seguridad cibernética, dentro de los límites de los mandatos respectivos de cada organización[1]. Con arreglo a ese memorando, la UNODC ha colaborado con la UIT para prestar asistencia técnica a los Estados que la solicitan. En ese contexto, la UNODC se ocupa en particular de los aspectos del delito cibernético relacionados con la prevención del delito y la justicia penal, mientras que la labor de la UIT va dirigida a mejorar la seguridad cibernética, incluso mediante la protección de la infraestructura crítica contra ataques computadorizados.

7. En su resolución 2011/33, titulada “Prevención, protección y cooperación internacional contra el uso de las nuevas tecnologías de la información para el abuso y/o explotación de los niños”, el Consejo Económico y Social solicitó a la UNODC que realizara un estudio que permitiera identificar, caracterizar y evaluar el impacto de las nuevas tecnologías de la información en el abuso y la explotación de los niños, tomando en cuenta datos pertinentes reunidos por el Grupo de expertos. En esa resolución, el Consejo solicitó también a la UNODC que diseñara y realizara una encuesta acerca de las necesidades de los Estados en materia de capacitación en el ámbito de la investigación de delitos cometidos contra niños utilizando las nuevas tecnologías de la información y las comunicaciones y, sobre la base de los resultados de dicha encuesta, elaborara un programa de capacitación y asistencia técnica que ayudara a los Estados Miembros a luchar más eficazmente contra esos delitos.

8. En 2011, y en el primer semestre de 2012, la UNODC comenzó a examinar la bibliografía para el estudio sobre la incidencia de las nuevas tecnologías de la información en el abuso y la explotación de niños y tomó medidas preparatorias con respecto a la encuesta de las necesidades en materia de capacitación. De conformidad con la resolución 2011/33 del Consejo Económico y Social, se presentará a la Comisión para su examen en su 23° período de sesiones, que se celebrará en 2014, un informe sobre la aplicación de esa resolución, incluidas las actividades relacionadas con el estudio.

9. En abril y mayo de 2012 la UNODC organizó cursos prácticos en Nairobi para 10 países de África oriental y meridional; en Beirut, para 12 países de Asia occidental; y en Bangkok, para 11 países de Asia sudoriental y meridional. Los cursos prácticos brindaron la oportunidad de obtener información sobre las necesidades en materia de asistencia técnica de esos países en la esfera del delito cibernético. También se puso de manifiesto que existía: a) una necesidad establecida de impartir capacitación básica a los responsables de la formulación de políticas y

[1] Véase www.itu.int/ITU-D/cyb/cybersecurity/docs/cybercrime.pdf.

de la toma de decisiones a fin de que se diera mayor prioridad a las cuestiones relacionadas con el delito cibernético; b) la necesidad de seguir diseñando mecanismos para la cooperación internacional tanto oficial como oficiosa entre las fuerzas del orden y los fiscales; c) la necesidad de proporcionar un mayor acceso a los programas y componentes informáticos forenses y a la capacitación en este aspecto con objeto de emprender investigaciones sobre delitos cibernéticos; y d) la necesidad de promover las alianzas entre los sectores público y privado para reforzar las medidas de prevención del delito cibernético. Sobre la base de los resultados de los talleres, la UNODC se ocupa en la actualidad de analizar opciones para la prestación de asistencia técnica en el marco del programa mundial contra el delito cibernético y en forma conjunta con los asociados competentes, incluida la UIT, a los países de África oriental y meridional.

10. Representantes de la UNODC asistieron a reuniones con los principales prestadores de servicios electrónicos del mundo para continuar avanzando hacia el logro del apoyo y la participación del sector privado en el programa mundial contra el delito cibernético. En el programa se ha previsto una cooperación estrecha con asociados del sector privado y organizaciones intergubernamentales competentes que permita la colaboración en apoyo de los programas de fomento de la capacidad. El programa se ha diseñado para facilitar las relaciones de trabajo entre las fuerzas del orden y las oficinas locales de los prestadores de servicios electrónicos más importantes del mundo, e incluye sesiones informativas dirigidas a agentes especializados en delitos cibernéticos a cargo de prestadores mundiales de servicios en las que se explican los procedimientos institucionales y los requisitos relativos a las debidas garantías procesales, así como la forma de facilitar la transmisión a las fuerzas del orden de información estratégica sobre amenazas generada por los prestadores de servicios de seguridad cibernética más importantes del mundo.

11. En febrero de 2012 se realizó una misión de evaluación inicial a Panamá, a solicitud del Gobierno de ese país, con miras a seguir fomentando la capacidad nacional en la lucha contra el delito cibernético. Organizada en forma conjunta por la sede de la UNODC y la Oficina Regional para América Central y el Caribe, la misión colaboró con un grupo de trabajo interdepartamental del Gobierno en el examen y la revisión del marco legislativo aplicable al delito cibernético. El grupo de trabajo, en el que participaron autoridades nacionales y dirigentes de opinión, así como entidades del sector privado, fue establecido con el cometido de elaborar legislación relativa al delito cibernético para Panamá. Se celebraron consultas con el fin de convenir en un planteamiento amplio y exhaustivo para luchar contra el delito cibernético en ese país. Las autoridades de Panamá también expresaron interés en la estrategia de cooperación entre la UIT y la UNODC y en el apoyo que podrían recibir para reforzar la defensa de la infraestructura crítica nacional.

12. Además, con miras a seguir fortaleciendo la cooperación y la sensibilización con respecto al delito cibernético, en 2012 la UNODC llevó a cabo un curso práctico en la República Islámica del Irán, en atención a una solicitud para que se impartiera capacitación sobre ese tipo de delito a 80 agentes del orden y funcionarios del Ministerio de Justicia. También se celebraron reuniones con el personal de la oficina local de INTERPOL, la policía encargada de la lucha contra el delito cibernético y miembros del poder judicial a fin de intensificar la cooperación mundial contra ese fenómeno.

# III. Actividades de la Oficina de las Naciones Unidas contra la Droga y el Delito encaminadas a fortalecer la cooperación con los Estados Miembros, las organizaciones intergubernamentales y el sector privado

13. Con objeto de seguir intensificando la cooperación contra el delito cibernético en todos los niveles, la UNODC continuó participando en calidad de observador en las consultas del Comité del Convenio sobre el delito cibernético, en el marco del Convenio sobre el delito cibernético, del Consejo de Europa, y en su conferencia anual "Octopus".

14. La UNODC participó asimismo como asociada en la Commonwealth Cybercrime Initiative, empeñándose en encontrar medios de mejorar la cooperación entre la propia UNODC y los asociados de la iniciativa. La UNODC participó además como observadora en el European Cybercrime Training and Education Group y cooperó con la Organización para la Seguridad y la Cooperación en Europa en el contexto de su reunión anual de expertos policiales.

# IV. Actividades de la Oficina de las Naciones Unidas contra la Droga y el Delito encaminadas a prestar apoyo al Grupo de expertos encargado de realizar un estudio exhaustivo sobre el delito cibernético[a]

15. La primera reunión del Grupo de expertos se celebró en Viena del 17 al 21 de enero de 2011. En ella el Grupo de expertos examinó y aprobó un conjunto de temas y una metodología para el estudio (véase E/CN.15/2011/19). La metodología contemplaba la distribución de un cuestionario a los Estados Miembros, a organizaciones intergubernamentales y a representantes del sector privado e instituciones académicas. De conformidad con la metodología acordada, la UNODC recopiló información durante el período de febrero a julio de 2012[2].

16. En junio de 2012 se envió un proyecto de cuestionario a todos los Estados Miembros para recabar sus observaciones. Una vez recibidas estas, la UNODC ultimó el cuestionario y lo difundió mediante el uso de un portal de reunión de datos basado en la web. Con objeto de confirmar con los Estados Miembros que eran correctos los aspectos de la información recopilada y analizada, la UNODC envió a cada Estado un resumen de sus disposiciones legislativas relativas al delito cibernético solicitándole sus observaciones y correcciones en caso necesario. En noviembre de 2012 la UNODC mantuvo consultas con los expertos designados por cada grupo regional acerca del análisis preliminar de los resultados recibidos a

---

[a] El texto de la sección IV fue publicado originalmente en un documento de antecedentes sin editar (UNODC/CCPCJ/EG.4/2013/2); el texto que figura en el presente informe es la versión editada conforme a las normas establecidas de la Secretaría.

[2] Se recibió información de 69 Estados Miembros con la siguiente distribución regional: África (11), América (13), Asia (19), Europa (24) y Oceanía (2). Se recibió información de 40 organizaciones del sector privado, 17 organizaciones académicas y 11 organizaciones intergubernamentales. La Secretaría también examinó más de 500 documentos de fuentes públicas.

partir del cuestionario al que habían contestado los Estados Miembros. Sobre la base de las respuestas al cuestionario recibidas de los Estados Miembros, el sector privado y organizaciones académicas e intergubernamentales, la UNODC preparó un proyecto de estudio para que lo examinara el Grupo de expertos.

17. La segunda reunión del Grupo de expertos se celebró del 25 al 28 de febrero de 2013[3]. En ella el Grupo de expertos tomó nota y efectuó un examen del estudio exhaustivo del delito cibernético que había preparado la UNODC con los auspicios del Grupo de expertos. El Grupo señaló que en sus deliberaciones, al igual que en el estudio, quedaban reflejadas las opiniones recopiladas y las diferentes estrategias adoptadas por los Estados para prevenir el delito cibernético y luchar contra ese fenómeno. En las deliberaciones sobre el estudio de referencia, se hizo notar que existía amplio apoyo en favor del fomento de la capacidad y de la asistencia técnica, así como del papel de la UNODC en ese sentido. Se expresaron distintas opiniones acerca del contenido, las conclusiones y las opciones que figuraban en el estudio. El Grupo de expertos analizó el camino a seguir y recomendó que la Comisión siguiera examinando el estudio en su 22° período de sesiones.

18. La UNODC se encargó de elaborar el resumen del estudio exhaustivo, que se proporciona a continuación, según lo había solicitado el Grupo de expertos. La UNODC preparó las conclusiones y opciones contenidas en el estudio y el resumen sobre la base de la información empírica facilitada y sin la intención de que constituyeran recomendaciones[4].

## A. Resumen del estudio exhaustivo del problema del delito cibernético elaborado por la Oficina de las Naciones Unidas contra la Droga y el Delito

### 1. La conectividad mundial y el delito cibernético

19. En 2011 al menos 2.300 millones de personas, es decir, aproximadamente un tercio de la población total del mundo, tenían acceso a Internet. Más del 60% de los usuarios estaban en países en desarrollo y el 45% tenían menos de 25 años. Se estima que, para 2017, las suscripciones a la banda ancha móvil llegarán, aproximadamente, al 70% de la población mundial. Para 2020 el número de dispositivos interconectados por la red (“Internet de las cosas”) será seis veces mayor al número de personas, lo que transformará la concepción actual de Internet. En el mundo hiperconectado del futuro será difícil imaginar un “delito informático”, o quizás un delito de cualquier otro tipo, que no implique pruebas electrónicas relacionadas con la conectividad del protocolo Internet.

20. Las definiciones del delito cibernético dependen, en gran medida, de la intención con que se emplee esa expresión. Un número limitado de actos contra la confidencialidad, la integridad y la disponibilidad de los datos o sistemas informáticos se hallan en la base del delito cibernético. Sin embargo, los actos relacionados con la informática realizados en provecho propio, o para obtener beneficios económicos o perjudicar económicamente a otros, por ejemplo los delitos

---

[3] El resultado de la reunión se describe en UNODC/CCPCJ/EG.4/2013/3.

[4] El estudio en su versión completa existe solo en inglés, y se hace referencia a él en E/CN.15/2013/CRP.5.

relacionados con la identidad, y los actos que guardan relación con contenidos informáticos (los cuales quedan comprendidos todos en el significado más amplio de la expresión “delito cibernético”), impiden llegar fácilmente a definiciones jurídicas de esa expresión en un sentido general. Es preciso establecer determinadas definiciones respecto de los actos que se hallan en la base del delito cibernético. No obstante, la definición de ese delito no reviste tanta importancia a otros fines, como la delimitación del alcance de las facultades especializadas de investigación y de cooperación internacional, que se centran con mayor eficacia en las pruebas electrónicas de cualquier delito, más que en un concepto amplio y artificial del “delito cibernético”.

### 2. Panorama mundial del delito cibernético

21. Para muchos países, el aumento vertiginoso de la conectividad mundial ha llegado en medio de cambios económicos y demográficos, con crecientes disparidades en los ingresos, ajustes en los gastos del sector privado y menos liquidez financiera. A nivel mundial, los funcionarios encargados de hacer cumplir la ley que respondieron al estudio consideraron que habían aumentado los delitos cibernéticos a medida que tanto personas como grupos delictivos organizados buscaban nuevas posibilidades ilícitas para obtener ganancias y beneficios personales. Se estima que más del 80% de esos actos tienen su origen en alguna forma de actividad organizada, con mercados negros cibernéticos establecidos en un círculo de creación de programas informáticos maliciosos, infección informática, gestión de redes zombi o “botnet”, recolección de datos personales y financieros, venta de datos y obtención de dinero a cambio de información financiera. Los delincuentes cibernéticos ya no necesitan pericia ni habilidades técnicas complejas. Especialmente en el contexto de los países en desarrollo han aparecido subculturas de jóvenes dedicados al fraude financiero relacionado con la informática, muchos de los cuales se inician en dicho delito en sus últimos años de adolescencia.

22. En todo el mundo, los actos delictivos cibernéticos están distribuidos, en términos generales, entre los actos motivados por intereses financieros y los relacionados con el contenido informático, así como aquellos que atentan contra la confidencialidad, la integridad y la accesibilidad de los sistemas informáticos. Sin embargo, los gobiernos y las empresas del sector privado perciben la amenaza y el riesgo relativos de manera diferente. En la actualidad las estadísticas de delitos registrados por la policía no son una base sólida para hacer comparaciones entre países, aunque suelen ser importantes para formular políticas a nivel nacional. Dos tercios de los países consideran que su sistema de estadísticas policiales es insuficiente para registrar los delitos cibernéticos. Las tasas de delitos cibernéticos registradas por la policía se corresponden con los niveles de desarrollo del país y con la capacidad policial especializada más que con las tasas de delincuencia existentes.

23. Las encuestas sobre victimización son una base más sólida de comparación. Demuestran que, en el caso de los delitos cibernéticos, la victimización individual es considerablemente superior a la que corresponde a las formas de delitos “convencionales”. Las tasas de victimización por fraude en línea con tarjetas de crédito, robo de identidad, respuesta a una tentativa de “pesca de datos” o “phishing”, o acceso no autorizado al correo electrónico varían entre el 1% y el 17% de la población con acceso a Internet de 21 países de todo el mundo, mientras que las tasas de delitos típicos, como robo, hurto y robo de coches, son en

esos mismos países inferiores al 5%. Las tasas de victimización en el caso de delitos cibernéticos son más altas en los países con menores niveles de desarrollo, lo que obliga a subrayar la necesidad de aumentar las medidas de prevención en esos países.

24. Las empresas del sector privado en Europa informan de tasas similares de victimización, entre el 2% y el 16%, en relación con actos como la violación de datos por intrusión o "phishing". Los mecanismos ilegales elegidos para cometer esos delitos, como por ejemplo las redes zombi o "botnet", tienen un alcance mundial. En 2011 había más de un millón de direcciones únicas del protocolo Internet en todo el mundo que funcionaban como servidores de mando y control de redes zombi o "botnet". El contenido de Internet también planteaba una importante preocupación a los gobiernos. Entre el material que se eliminaba estaban no solo la pornografía infantil y los discursos de incitación al odio, sino también el contenido relacionado con la difamación y las críticas al gobierno, lo que en algunos casos despertaba inquietudes respecto de los derechos humanos. Se estima que casi el 24% del tráfico total de Internet a nivel mundial infringe los derechos de propiedad intelectual, con descargas de material entre pares (P2P) especialmente numerosas en países de África, América del Sur y Asia occidental y meridional.

### 3. Legislación relativa al delito cibernético

25. Las medidas legales desempeñan un papel fundamental en la prevención del delito cibernético y en la lucha contra ese fenómeno. Son necesarias en todas las esferas, entre ellas la tipificación como delito, la competencia procesal, la jurisdicción, la cooperación internacional y la responsabilidad de los proveedores de servicios de Internet. A nivel nacional, la legislación vigente y la legislación nueva (o prevista) sobre los delitos cibernéticos suelen centrarse en su tipificación como delito, lo que indica un interés predominante en establecer figuras delictivas específicas de los principales actos que constituyen delitos cibernéticos. Sin embargo, los países cada vez reconocen más la necesidad de contar con legislación en otras esferas. En comparación con la legislación vigente, la legislación nueva o prevista en esta materia trata principalmente de las medidas de investigación, la jurisdicción, las pruebas electrónicas y la cooperación internacional. A nivel mundial, menos de la mitad de los países que respondieron consideraron que su ordenamiento jurídico en materia penal y procesal era suficiente, aunque esto oculta grandes diferencias regionales. Más de los dos tercios de los países de Europa comunicaron legislación suficiente, pero la situación era totalmente contraria en África, América, Asia y Oceanía, donde más de los dos tercios de los países consideraron que la legislación era parcialmente suficiente o no lo era en absoluto. Solo la mitad de los países que comunicaron que su legislación era insuficiente también señalaron legislación nueva o prevista, lo que obliga a destacar la urgente necesidad de consolidar las disposiciones legislativas en esas regiones.

26. En el último decenio se han producido grandes avances en la promulgación de instrumentos internacionales y regionales destinados a hacer frente al delito cibernético. Esos instrumentos pueden ser vinculantes o no. Se pueden definir cinco grupos, que consisten en instrumentos elaborados o inspirados por: a) el Consejo de Europa o la Unión Europea, b) la Comunidad de Estados Independientes o la Organización de Cooperación de Shanghái, c) organizaciones intergubernamentales africanas, d) la Liga de los Estados Árabes y e) las Naciones Unidas. Existe una

considerable interdependencia entre todos los instrumentos, en especial conceptos y enfoques elaborados en el marco del Convenio sobre el delito cibernético, del Consejo de Europa. Del análisis de los artículos de 19 instrumentos multilaterales pertinentes al delito cibernético se desprende la existencia de disposiciones fundamentales comunes, pero también hay considerables diferencias en las esferas sustantivas que tratan.

27. A nivel mundial, 82 países han firmado o ratificado un instrumento vinculante sobre el delito cibernético[5]. Además de propiciar una adhesión oficial y la aplicación de sus disposiciones, los instrumentos multilaterales sobre el delito cibernético han influido en las legislaciones nacionales en forma indirecta, al ser utilizados como modelo por Estados que no son partes en ellos o mediante la influencia ejercida por las leyes de los Estados parte en otros países. La adhesión a un instrumento multilateral sobre el delito cibernético coincide con la percepción de una mayor suficiencia de las leyes nacionales penales y procesales, lo que indica que, generalmente, las disposiciones multilaterales vigentes en la materia se consideran eficaces. En opinión de los más de 40 países que suministraron información, el Convenio sobre el delito cibernético, del Consejo de Europa, fue el instrumento multilateral más utilizado para elaborar legislación sobre este tema. Aproximadamente en la mitad de ese total de países se utilizaban instrumentos multilaterales de otros “grupos”.

28. En general, un tercio de los países que respondieron comunicaron que su legislación armonizaba en gran medida, o en muy alto grado, con la de los países considerados importantes a los fines de la cooperación internacional. Esta respuesta variaba, no obstante, según la región, con mayores índices de armonización dentro de América y Europa. Esto puede deberse al uso, en algunas regiones, de instrumentos multilaterales, inherentemente diseñados para desempeñar un papel en la armonización. La fragmentación a nivel internacional y la diversidad de leyes nacionales, por lo que respecta a los actos tipificados como delitos cibernéticos, las formas de atribución de la jurisdicción y los mecanismos de cooperación, pueden tener relación con la existencia de múltiples instrumentos sobre el delito cibernético con diferente alcance temático y geográfico. Tanto los instrumentos como las regiones presentan en la actualidad divergencias derivadas de diferencias jurídicas y constitucionales subyacentes, como por ejemplo diferentes concepciones de los derechos y de la privacidad.

### 4. Tipificación del delito

29. La información sobre las normas penales relativas a los delitos cibernéticos se reunió mediante el cuestionario del estudio y mediante el análisis de fuentes primarias de la legislación disponible recopilada por la Secretaría[6]. El cuestionario del estudio mencionaba 14 actos comúnmente incluidos en el concepto de delito

---

[5] Uno o más de los siguientes instrumentos: el Convenio sobre el delito cibernético, del Consejo de Europa; la Arab Convention on Combating Information Technology Offences (Liga de los Estados Árabes); el Acuerdo sobre la Cooperación entre los países de la CEI para luchar contra el delito en la esfera de la información computadorizada; o el Agreement in the Field of International Information Security (Organización de Cooperación de Shanghái).

[6] Se analizaron las fuentes primarias de la legislación correspondiente a 97 Estados Miembros, incluidos 56 que respondieron al cuestionario, con la siguiente distribución regional: África (15), América (22), Asia (24), Europa (30) y Oceanía (6).

cibernético[7]. Los países que respondieron mostraron una tipificación generalizada de estos 14 actos, con excepción, principalmente, de los delitos relativos al correo basura y, en menor medida, los delitos relativos a los dispositivos de uso indebido, el racismo y la xenofobia, y la incitación a la prostitución o seducción de menores en línea. Esto refleja un cierto consenso básico sobre lo que constituye una conducta culpable en la esfera de la informática. Los países comunicaron pocos delitos además de los mencionados en el cuestionario. Estos se referían principalmente al contenido informático, incluidos el material obsceno, el juego en línea y los mercados ilícitos en línea, como el mercado de drogas y de personas. Para los 14 actos los países comunicaron la existencia de delitos cibernéticos específicos correspondientes a actos básicos contra la confidencialidad, la integridad y la accesibilidad de los sistemas informáticos. Para otras formas de delitos cibernéticos se aplicaban con más frecuencia figuras delictivas generales (no específicamente cibernéticas). Sin embargo, se comunicó que en el caso de los actos relacionados con la informática que implicaban una violación de la privacidad, un fraude o falsificación o un delito contra la identidad se aplicaban ambos criterios.

30. Si bien existe un consenso de alto nivel con respecto a amplias esferas de la tipificación, un análisis detallado de las disposiciones de las legislaciones nacionales muesta que existen distintos criterios. Los delitos que implican un acceso ilícito a los sistemas y los datos informáticos difieren con respecto al objeto del delito (datos, sistema o información) y respecto a la tipificación del “mero” acceso o el requisito adicional de la intención, por ejemplo la intención de causar una pérdida o daño. El requisito de la intención para la existencia del delito también difiere en los criterios de tipificación de la interferencia de datos o sistemas informáticos. La mayoría de los países requieren que la interferencia sea intencional, mientras que otros incluyen la interferencia temeraria. En el caso de la interferencia de datos informáticos, la figura delictiva va de dañar o borrar hasta alterar, suprimir, agregar o transmitir datos. La figura de la interceptación ilícita difiere según esté limitada o no a las transmisiones de datos no públicos y según esté limitada o no a la interceptación “por medios técnicos”. No todos los países tipifican como delito los dispositivos informáticos de uso indebido. Entre los que sí lo hacen, las diferencias estriban en que la figura abarque la posesión, difusión o uso de programas informáticos (por ejemplo, el malware) o de códigos de acceso informático (por ejemplo, la contraseña de la víctima). Desde la perspectiva de la cooperación internacional, estas diferencias pueden tener consecuencias para el caso de que se dictamine la doble incriminación entre países.

31. Varios países han establecido figuras delictivas cibernéticas específicas para el fraude, la falsificación y los delitos contra la identidad relacionados con la

[7] Acceso ilegal a un sistema informático; acceso, interceptación o adquisición ilícitas de datos informáticos; interferencia ilícita de datos o de sistemas; producción, distribución o posesión de dispositivos informáticos de uso indebido; violación de la privacidad o de las medidas de protección de los datos; fraude o falsificación relacionados con la informática; delitos contra la identidad relacionados con la informática; delitos contra la propiedad intelectual o las marcas de fábrica relacionados con la informática; actos relacionados con la informática que causen daños personales; actos relacionados con la informática que impliquen racismo o xenofobia; producción, distribución o posesión relacionados con la informática de pornografía infantil; incitación a la prostitución o seducción de menores relacionada con la informática; y actos relacionados con la informática en favor del terrorismo.

informática. Otros han extendido el ámbito de aplicación de las disposiciones generales sobre fraude o robo o han recurrido a delitos que abarcan los elementos constitutivos, como el acceso ilícito, la interferencia y la falsificación de datos, en el caso de los delitos contra la identidad. Varias figuras delictivas relacionadas con el contenido, especialmente las relativas a la pornografía infantil, muestran una generalizada tipificación como delitos. Sin embargo, aparecen diferencias con respecto a la definición de "menor", las limitaciones en relación con el material "visual" o la exclusión del material simulado, como también respecto a los actos abarcados. En el caso de la pornografía infantil, por ejemplo, si bien la gran mayoría de los países incluyen su producción y distribución, existe una mayor variación con respecto a la tipificación como delito de la posesión y el acceso. Por lo que se refiere a los delitos relacionados con la informática en violación de los derechos intelectuales o las marcas de fábrica, los países comunicaron, en general, la aplicación de los delitos generales para los actos cometidos con dolo y a escala comercial.

32. El creciente uso de las redes sociales y del contenido de Internet generado por los usuarios ha dado lugar a respuestas normativas de los gobiernos, incluso la aplicación del derecho penal, y a llamamientos en favor del respeto de los derechos a la libertad de expresión. Los países que respondieron aplicaban diferentes limitaciones de esos derechos, incluso con respecto a la difamación, el desacato, las amenazas, la incitación al odio, el insulto a las creencias religiosas, el material obsceno y la subversión del Estado. El elemento sociocultural de algunas limitaciones se refleja no solo en la legislación nacional sino también en instrumentos multilaterales. Algunos instrumentos regionales sobre el delito cibernético, por ejemplo, contienen figuras delictivas amplias con respecto al atentado contra la moral pública y los principios o valores familiares o religiosos, como también acerca del material pornográfico.

33. Las normas internacionales de derechos humanos actúan al mismo tiempo como espada y como escudo al requerir la tipificación como delito de (ciertas) formas extremas de expresión y proteger a la vez otras formas. Por lo tanto, los Estados que son parte en los instrumentos internacionales de derechos humanos pertinentes deben imponer algunas prohibiciones a la libertad de expresión, incluida la incitación al genocidio, la manifestación de odio que constituye una incitación a la discriminación, la hostilidad o la violencia, la incitación al terrorismo y la propaganda de guerra. Para otros países, el "margen de apreciación" les permite una cierta libertad para determinar límites a la libertad de expresión que sean aceptables para sus propias culturas y tradiciones jurídicas. De todas formas, las normas internacionales de derechos humanos intervendrán en un cierto punto. Por ejemplo, las leyes penales sobre difamación, desacato a la autoridad e insulto, que se aplican a las expresiones en línea tendrán un alto umbral para demostrar que las medidas son proporcionadas, apropiadas y lo menos invasivas posibles. Cuando el contenido sea ilegal en un país al tiempo que su producción y difusión sean lícitas en otro, los Estados tendrán que centrar las respuestas de la justicia penal en las personas que tienen acceso al contenido dentro de la jurisdicción nacional y no en el contenido producido fuera del país.

### 5. Mantenimiento del orden e investigaciones

34. Más del 90% de los países que respondieron señalaron que las autoridades encargadas de aplicar la ley solían tomar conocimiento de los actos delictivos

cibernéticos por denuncias de las víctimas, ya fueran personas a título individual o empresas. Los países que respondieron estimaron que la tasa real de victimización denunciada a la policía por delitos cibernéticos era superior al 1%. Una encuesta mundial del sector privado sugiere que el 80% de las personas víctimas de los principales delitos cibernéticos no denuncia el hecho a la policía. La escasez de denuncias se debe a una falta de conocimiento de la victimización y de los mecanismos de denuncia, a la vergüenza y el bochorno de la víctima y a los posibles riesgos para la reputación de las empresas. Las autoridades de todas las regiones del mundo destacaron las iniciativas para favorecer las denuncias, entre ellas los sistemas de denuncias en línea y líneas telefónicas directas, las campañas de sensibilización pública, los enlaces con el sector privado y mayores actividades de divulgación e intercambio de información por parte de la policía. Sin embargo, la respuesta a los delitos cibernéticos en caso de denuncia de un incidente debe estar acompañada por investigaciones tácticas a mediano y largo plazo que se centren en el mercado del delito y en los arquitectos de los planes delictivos. En los países desarrollados, las fuerzas del orden realizan estas tareas, incluso mediante brigadas de agentes secretos que buscan delincuentes en los sitios de las redes sociales, las salas de charla y los servicios de mensajería instantánea y P2P. Los problemas en la investigación de los delitos cibernéticos nacen de las innovaciones delictivas de los autores, de las dificultades en acceder a las pruebas electrónicas y de las limitaciones en materia de recursos internos, capacidad y logística. Los sospechosos suelen utilizar tecnologías de anonimato y de confusión, y las nuevas técnicas se difunden rápidamente a una amplia audiencia criminal mediante los mercados del delito en línea.

35. Para las investigaciones sobre delitos cibernéticos que emprenden las fuerzas del orden se necesita una mezcla de técnicas policiales tradicionales y nuevas. Mientras que algunas diligencias investigativas se pueden realizar con las facultades tradicionales, muchas disposiciones procesales con un enfoque espacial y orientado hacia los objetos no se adaptan de manera satisfactoria a otro que implica el almacenamiento de datos electrónicos y flujos de datos en tiempo real. El cuestionario del estudio remitía a 10 diligencias investigativas de los delitos cibernéticos, que iban de la inspección e incautación genéricas a las facultades especializadas, como la conservación de datos informáticos[8]. Con mayor frecuencia los países comunicaron la existencia de facultades generales (no específicas de la cibernética) para todas las diligencias investigativas. Varios países también se refirieron a una legislación específica de la cibernética, especialmente para garantizar la conservación rápida de datos informáticos y para obtener datos almacenados por un suscriptor. Muchos países informaron de que carecían de competencia jurídica para diligencias novedosas como los instrumentos remotos para los estudios forenses. Aunque las competencias procesales tradicionales pueden aplicarse a situaciones en la esfera de la cibernética, en muchos casos este criterio también puede llevar a una incertidumbre jurídica y a que se cuestione la licitud en

[8] Inspección de equipo o datos; incautación de equipo o datos informáticos; requerimiento de información del suscriptor; requerimiento de los datos almacenados relativos al tráfico; requerimiento de los datos almacenados relativos al contenido; recopilación en tiempo real de datos relativos al tráfico; recopilación en tiempo real de los datos sobre el contenido; conservación rápida de datos informáticos almacenados; empleo de instrumentos remotos en los estudios forenses; y acceso transfronterizo a un sistema o datos informáticos.

la obtención de las pruebas y, por lo tanto, su admisibilidad. En general, entre los criterios nacionales hay menos elementos básicos en común en relación con las facultades investigativas en el caso de los delitos cibernéticos que con la tipificación como delito de muchos actos cibernéticos.

36. Independientemente de la forma legal que tengan las facultades investigativas, todas las autoridades que respondieron emplean la inspección e incautación para la apropiación física del equipo de computación y la captura de los datos informáticos. La mayoría de los países también emplean requerimientos para obtener de los proveedores de servicios de Internet los datos informáticos almacenados. Sin embargo, fuera de Europa, alrededor de un tercio de los países señalaron que tenían problemas para obligar a los terceros en una investigación a facilitar información. Aproximadamente las tres cuartas partes de los países recurren a diligencias investigativas especializadas, como la obtención en tiempo real de datos o la conservación rápida de datos. El empleo de diligencias investigativas requiere generalmente un mínimo de pruebas iniciales o la denuncia de un hecho delictivo cibernético. Para las diligencias más invasivas, como las que implican la obtención en tiempo real de datos o el acceso al contenido de los datos, se suelen exigir mayores requisitos, como aportar pruebas de la comisión de un hecho grave o demostrar la existencia de causa probable o motivos fundados.

37. La relación entre las fuerzas del orden y los proveedores de servicios de Internet es especialmente compleja. Los proveedores de servicios tienen información de los suscriptores, facturas, algunos registros de conexión, información sobre la ubicación (como datos de las torres de celulares para los proveedores de telefonía móvil) y el contenido de las comunicaciones, todo lo cual puede representar una prueba electrónica fundamental de un delito. Las obligaciones jurídicas nacionales y las políticas de retención y divulgación de datos del sector privado varían enormemente según el país, la industria y el tipo de datos. En general, los países informaron de que empleaban una orden judicial para obtener pruebas de los proveedores de servicios. Sin embargo, en algunos casos las fuerzas del orden pueden obtener en forma directa datos almacenados del suscriptor, datos sobre el tráfico e incluso datos sobre el contenido. A este respecto, muchas organizaciones del sector privado afirmaron que, como política básica, exigían el debido proceso legal para divulgar la información, pero que también cumplían voluntariamente las solicitudes directas de las fuerzas del orden en determinadas circunstancias. La relación oficiosa entre las fuerzas del orden y los proveedores de servicios, que existe en más de la mitad de los países que respondieron, facilita el proceso de intercambio de información y fomento de la confianza. En las respuestas se indicó la necesidad de equilibrar la privacidad y el debido proceso con la divulgación de las pruebas en forma oportuna a fin de garantizar que el sector privado no se convirtiera en un cuello de botella de las investigaciones.

38. La investigación de los delitos cibernéticos implica invariablemente cuestiones de privacidad en el marco de la normativa internacional de derechos humanos. Estas normas de derechos humanos estipulan que las leyes deben ser suficientemente claras para dar una indicación adecuada de las circunstancias en que las autoridades están facultadas para realizar una diligencia investigativa, y especifican que deben existir garantías suficientes y eficaces contra el abuso. Los países comunicaron que protegían el derecho a la privacidad en la legislación nacional y que también existía una serie de límites y de salvaguardias en cuanto a las investigaciones. Sin embargo,

cuando las investigaciones son transnacionales, los distintos niveles de protección tornan imprevisible el acceso de las fuerzas del orden extranjeras a los datos y dan lugar a posibles lagunas jurisdiccionales en los regímenes de protección de la privacidad.

39. Más del 90% de los países que respondieron al cuestionario habían comenzado a establecer estructuras especializadas para la investigación de los delitos cibernéticos y de los delitos que generan pruebas electrónicas. Sin embargo, en los países en desarrollo esas estructuras no disponían de los recursos suficientes y padecían de una escasez de capacidad. Los países con un menor nivel de desarrollo contaban con un número mucho menor de agentes de policía especializados, aproximadamente 0,2 por cada 100.000 usuarios nacionales de Internet. Este porcentaje era de dos a cinco veces mayor en países más desarrollados. Se comunicó que en los países menos desarrollados el 70% de los agentes del orden especializados carecía de conocimientos y de equipo de informática, y solamente la mitad recibía capacitación más de una vez por año. Más de la mitad de los países de África que respondieron, y un tercio de los países de América, comunicaron que los recursos de las fuerzas del orden para investigar los delitos cibernéticos eran insuficientes. Es posible que, a nivel mundial, el panorama sea aún peor. El estudio recibió respuestas, por ejemplo, de solo el 20% de los 50 países menos adelantados del mundo. Todos los países de África que respondieron, y más del 80% de los países de América y de Asia y Oceanía, comunicaron que necesitaban asistencia técnica. El sector que se citaba con más frecuencia como necesitado de asistencia técnica fue el de las técnicas generales de investigación de delitos cibernéticos. El 60% de los países que requerían asistencia señalaron que la necesitaban los organismos encargados de hacer cumplir la ley.

### 6. Pruebas electrónicas y respuesta de la justicia penal

40. La prueba es el medio de constatar los hechos que hacen a la culpabilidad o inocencia de una persona en un juicio. La prueba electrónica consiste en cualquier material de ese tipo que exista en forma electrónica o digital. Puede estar almacenado o ser transitorio. Puede existir en forma de archivos informáticos, transmisiones, registros, metadatos o datos de la red. La ciencia forense digital se ocupa de recuperar información, frecuentemente volátil y fácilmente contaminada, que pueda tener valor probatorio. Entre las técnicas forenses se encuentran la creación de copias exactas (*bit por bit*) de la información almacenada y borrada, el bloqueo de escritura para asegurarse de que la información original no sea cambiada y el resumen criptográfico del archivo (*hashes*) o firmas digitales que pueda mostrar los cambios en la información. Casi todos los países comunicaron que tenían algún tipo de capacidad en ciencias forenses digitales. Sin embargo, muchos países que respondieron, de todas las regiones, señalaron que tenían un número insuficiente de técnicos forenses, diferencias entre la capacidad a nivel federal y estatal, falta de instrumentos forenses y retrasos debidos a la abrumadora cantidad de datos para analizar. La mitad de los países comunicaron que los sospechosos empleaban claves secretas, con lo cual el acceso a este tipo de pruebas era difícil y muy lento cuando no se conocía la clave. En la mayoría de los países la tarea de analizar las pruebas electrónicas correspondía a los organismos policiales. No obstante, los fiscales deben ver y comprender las pruebas electrónicas para poder presentar la acusación. Todos los países de África y un tercio de los países de otras regiones comunicaron que los recursos que tenían eran insuficientes para que los fiscales pudieran realizar

esa tarea. En general, los fiscales tenían menos conocimientos informáticos que los investigadores. Alrededor del 65% de los países de todo el mundo que respondieron mencionaron que los fiscales tenían alguna forma de especialización en delitos cibernéticos. Solamente el 10% de los países comunicaron que contaban con servicios judiciales especializados. La vasta mayoría de los casos de delitos cibernéticos estaba en manos de jueces no especializados que, en el 40% de los países que respondieron, no recibían ninguna forma de capacitación relacionada con los delitos cibernéticos. La capacitación judicial en derecho cibernético, recopilación de pruebas e informática básica y avanzada constituía una prioridad especial.

41. Más del 60% de los países que respondieron no hacían una distinción jurídica entre prueba electrónica y prueba física. Si bien los criterios eran variados, muchos países consideraban que esa era una buena práctica, ya que garantizaba una admisibilidad equitativa junto a los otros tipos de pruebas. Varios países fuera de Europa no admitían las pruebas electrónicas en absoluto, con lo que resultaba imposible el procesamiento en caso de un delito cibernético o de cualquier otro delito que se debiera probar con información electrónica. Si bien los países no contaban, en general, con normas propias para las pruebas electrónicas, una serie de países se remitieron a principios como la norma de la mejor prueba, la pertinencia de la prueba, la norma de la prueba indirecta, la autenticidad y la integridad, todo lo cual podría resultar especialmente pertinente en lo que respecta a las pruebas electrónicas. Muchos países destacaron los problemas que surgían para atribuir un hecho a una determinada persona y señalaron que esto dependía muchas veces de pruebas circunstanciales.

42. Los problemas que encuentran tanto los investigadores de las fuerzas del orden como los fiscales se traducen en que las tasas de enjuiciamiento son bajas en el caso de los delincuentes cibernéticos. El número de sospechosos identificados por el registro policial en el caso de delitos de pornografía infantil es comparable al registrado en relación con otros delitos sexuales; sin embargo, solo aproximadamente en 25 de cada 100 casos de delitos como el acceso ilegal y el fraude o la falsificación relacionados con la informática se logra identificar a los sospechosos. Muy pocos países pudieron facilitar datos sobre las personas encausadas o condenadas. Sin embargo, los cálculos correspondientes a los delitos cibernéticos en un país mostraron que el porcentaje de personas condenadas en relación con los delitos registrados era considerablemente menor al porcentaje correspondiente a los delitos “convencionales”.

### 7. Cooperación internacional

43. Los países que respondieron al cuestionario del estudio señalaron que entre el 30% y el 70% de los delitos cibernéticos tenían una dimensión transnacional, con lo cual se planteaban cuestiones de investigaciones transnacionales, soberanía, jurisdicción, pruebas extraterritoriales y requerimientos de cooperación internacional. La dimensión transnacional de un delito cibernético se presenta cuando un elemento o un efecto considerable del delito se dan en otro territorio, o cuando parte del *modus operandi* está en otro territorio. El derecho internacional establece distintas bases para la atribución de la jurisdicción aplicable a estos actos, como la jurisdicción según el territorio y la jurisdicción según la nacionalidad. Algunas de estas normas también figuran en instrumentos multilaterales sobre el

delito cibernético. Mientras que todos los países de Europa consideran que el derecho nacional brinda un marco suficiente para la tipificación del delito cibernético y para el enjuiciamiento en caso de actos extraterritoriales, entre un tercio y más de la mitad de los países de otras regiones del mundo señalan marcos jurídicos insuficientes. En muchos países las disposiciones reflejan la idea de que no hace falta que "todo" el acto delictivo se realice dentro de un país para afirmar la jurisdicción territorial. Se pueden establecer vínculos territoriales con respecto a los elementos o efectos del acto, o a la ubicación de los sistemas o datos informáticos empleados en la comisión del delito. Cuando se plantea un conflicto jurisdiccional, generalmente se resuelve con consultas oficiales u oficiosas entre los países. Las respuestas de los países no indican, en la actualidad, ninguna necesidad de contar con formas adicionales de jurisdicción sobre una presunta dimensión del "ciberespacio". Más bien las formas de jurisdicción según la territorialidad o según la nacionalidad casi siempre permiten establecer una relación suficiente entre los actos delictivos cibernéticos y al menos un Estado.

44. Las formas de cooperación internacional incluyen la extradición, la asistencia judicial recíproca, el reconocimiento recíproco de la sentencia extranjera y la cooperación oficiosa entre policía y policía. Debido al carácter volátil de la prueba electrónica, la cooperación internacional en asuntos penales en la esfera de los delitos cibernéticos requiere una respuesta pronta y la habilidad de solicitar diligencias investigativas especializadas, como la conservación de los datos informáticos. El recurso a formas tradicionales de cooperación es lo más usual para obtener pruebas extraterritoriales en los casos de delincuencia cibernética, ya que más del 70% de los países señalan que emplean para este fin solicitudes oficiales de asistencia judicial recíproca. Dentro de este tipo de cooperación oficial, casi el 60% de las solicitudes se fundan en instrumentos bilaterales. Los instrumentos multilaterales sirven de fundamento en el 20% de los casos. Se comunicó que el tiempo de respuesta en el caso de los mecanismos oficiales era de meses, tanto para la extradición como para la solicitud de asistencia judicial recíproca, un plazo que presenta un problema para la recopilación de pruebas electrónicas volátiles. El 60% de los países de África, América y Europa, y el 20% de Asia y Oceanía, afirmaron que existían canales para las solicitudes urgentes. Sin embargo, no estaba claro qué consecuencias tenía esto para el plazo de respuesta. Aproximadamente dos tercios de los países que respondieron admitían modos oficiosos de cooperación, aunque pocos países tenían una política para el empleo de esos mecanismos. Las iniciativas para una cooperación oficiosa y para facilitar la cooperación oficial, como por ejemplo redes accesibles las 24 horas del día, los 7 días de la semana, presentan grandes posibilidades de lograr respuestas más rápidas. Sin embargo, se utilizan muy poco, ya que se recurre a ellas en el 3% del total de los casos de delitos cibernéticos manejados por las fuerzas del orden del grupo de países que respondieron.

45. Se han previsto modos oficiales y oficiosos de cooperación que guían el procedimiento de lograr el consentimiento de un Estado para que fuerzas del orden extranjeras realicen investigaciones que afectan su soberanía. Sin embargo, cada vez más los investigadores, a sabiendas o no, acceden a datos extraterritoriales, al reunir pruebas, sin el consentimiento del Estado donde se encuentran físicamente los datos. Una de las razones de que se presente esta situación es la informática en la nube, que implica el almacenamiento de los datos en múltiples centros de datos situados en diferentes ubicaciones geográficas. La "ubicación" de los datos, si bien es

técnicamente posible de conocer, es cada vez más artificial, al grado de que las solicitudes tradicionales de asistencia judicial recíproca suelen dirigirse al país sede del proveedor del servicio más que al país donde el centro de datos está físicamente ubicado. El acceso directo de fuerzas del orden extranjeras a datos extraterritoriales puede ocurrir cuando los investigadores aprovechan una conexión activa desde un dispositivo del sospechoso o cuando emplean credenciales de acceso a los datos obtenidas legalmente. Los investigadores pueden, ocasionalmente, obtener datos de los proveedores de servicios extraterritoriales presentando una solicitud directa oficiosa, aunque los proveedores de servicios suelen requerir que se siga el debido proceso legal. Las disposiciones vigentes relativas al acceso "transfronterizo" contenidas en el Convenio sobre el delito cibernético, del Consejo de Europa, y la Convention on Information Technology Offences, de la Liga de los Estados Árabes, no regulan debidamente estas situaciones porque se centran en el "consentimiento" de la persona legalmente facultada para divulgar los datos y presuponen que se conocía la ubicación de los datos al momento de acceso o recepción.

46. El actual panorama de cooperación internacional corre el peligro de que aparezcan grupos de países que tengan las facultades y los procedimientos necesarios para cooperar entre ellos pero que, con respecto a los demás países, se limiten a emplear modos "tradicionales" de cooperación internacional que no toman en cuenta la especificidad de las pruebas electrónicas ni el carácter mundial de la delincuencia cibernética. Esto ocurre especialmente en el caso de la cooperación en las diligencias investigativas. La falta de un criterio común, incluso en los instrumentos multilaterales vigentes sobre el delito cibernético, significa que la solicitud de acciones, como por ejemplo la rápida conservación de los datos, será difícil de cumplir fuera de los países que tienen obligaciones internacionales de garantizar este servicio y de brindarlo cuando se solicite. La inclusión de esta facultad en el proyecto de convenio sobre la seguridad cibernética de la Unión Africana sería un adelanto en el camino de cubrir esta laguna. A nivel mundial, las divergencias en el alcance de las disposiciones sobre cooperación contenidas en los instrumentos multilaterales y bilaterales, la falta de obligación en el cumplimiento de los plazos, la falta de acuerdo sobre el acceso directo a los datos extraterritoriales, múltiples redes oficiosas de organismos encargados de hacer cumplir la ley y diversidad en las garantías de cooperación representan grandes obstáculos para lograr una cooperación internacional eficaz con respecto a las pruebas electrónicas en asuntos penales.

## 8. Prevención del delito cibernético

47. La prevención del delito comprende estrategias y medidas tendientes a reducir el riesgo de comisión de delitos y mitigar las posibles consecuencias perjudiciales para las personas y la sociedad. Casi el 40% de los países que respondieron dijeron que contaban con leyes o políticas nacionales para prevenir el delito cibernético. Otro 20% de los países se encontraba en el proceso de preparación de iniciativas en ese sentido. Los países destacaron que entre las buenas prácticas de prevención del delito cibernético figuraban la promulgación de leyes, una dirección eficaz, el fomento de la capacidad en el ámbito de la justicia penal y el mantenimiento del orden, la educación y la sensibilización, el desarrollo de una base firme de conocimientos y la cooperación entre los gobiernos, las comunidades y el sector privado, como también a nivel internacional. Más de la mitad de los países comunicaron la existencia de estrategias en materia de delito cibernético. En

muchos casos, esas estrategias estaban estrechamente integradas en las estrategias de seguridad cibernética. Aproximadamente el 70% de todas las estrategias nacionales comunicadas incluían componentes de sensibilización, cooperación internacional y capacidad de mantenimiento del orden. A los fines de la coordinación, los organismos que se señalaron con más frecuencia como las principales instituciones en materia de delitos cibernéticos fueron las fuerzas del orden y el ministerio público.

48. Las encuestas, incluidas las realizadas en países en desarrollo, demuestran que hoy en día la mayoría de los usuarios de Internet adoptan medidas básicas de seguridad. Los gobiernos, las entidades del sector privado y las instituciones académicas que respondieron a dichas encuestas destacaron la importancia de las campañas de sensibilización pública, en particular las relativas a las nuevas amenazas y las dirigidas a destinatarios específicos, como los menores. La educación de los usuarios resulta extremadamente eficaz cuando se combina con sistemas que los ayudan a alcanzar sus objetivos de manera segura. Si el costo para los usuarios es superior a su beneficio directo, estos tendrán pocos incentivos para adoptar medidas de seguridad. Las entidades del sector privado comunicaron que la sensibilización del usuario y del empleado debía integrarse en un enfoque integral de la seguridad. Los principios fundamentales y las buenas prácticas mencionadas incluían la responsabilidad de adoptar medidas sobre sensibilización, políticas y prácticas de gestión de riesgo, liderazgo a nivel de directorio y capacitación del personal. Los dos tercios de quienes respondieron por el sector privado habían realizado una evaluación de riesgos en materia de delitos cibernéticos y la mayoría comunicaron que usaban tecnologías de seguridad como cortafuegos, conservación de las pruebas digitales, identificación del contenido, detección de la intrusión y sistemas de supervisión y vigilancia. Sin embargo, se expresó la preocupación por el hecho de que las empresas pequeñas y medianas no adoptaran suficientes medidas para proteger los sistemas o bien tenían la impresión errónea de que no se convertirían en blanco de tales delitos.

49. Los marcos regulatorios tienen una importante función que desempeñar en la prevención del delito cibernético, tanto con respecto al sector privado en general como con respecto a los proveedores de servicio en particular. Casi la mitad de los países han dictado normas de protección de los datos, con requisitos específicos para la protección y el uso de los datos personales. Algunos de estos regímenes incluyen requisitos específicos para los proveedores de servicios de Internet y demás proveedores de comunicaciones electrónicas. Si bien las normas de protección de los datos requieren que los datos personales se borren cuando ya no sean necesarios, algunos países han establecido excepciones a los fines de la investigación penal, exigiendo que los prestadores de servicios de Internet almacenen tipos específicos de datos por un plazo determinado. Muchos países desarrollados también tienen normas que exigen a las organizaciones notificar las violaciones de datos a los particulares y a quienes dictan las normas. Los proveedores de servicios de Internet tienen generalmente una responsabilidad limitada como “meros conductores” de datos. La modificación del contenido trasmitido aumenta la responsabilidad, al igual que el conocimiento real o inferido de una actividad ilegal. La acción rápida después de la notificación, por otra parte, reduce la responsabilidad. Si bien existen posibilidades técnicas de que los proveedores de servicios filtren el contenido de Internet, las restricciones del acceso a Internet quedan sujetas a requisitos de previsibilidad y proporcionalidad en el

marco de las normas internacionales de derechos humanos que protegen el derecho a buscar, recibir y dar información.

50. La alianza entre los sectores público y privado es fundamental para la prevención del delito cibernético. Más de la mitad de los países señalaron la existencia de alianzas. Estas se habían creado en igual número por acuerdos oficiosos y por normas legales. Las entidades del sector privado eran las que más participaban, seguidas por las instituciones académicas y las organizaciones internacionales y regionales. Las alianzas se utilizaban generalmente para facilitar el intercambio de información sobre amenazas y tendencias, pero también para desarrollar actividades y medidas de prevención en casos específicos. En el contexto de algunas alianzas entre el sector público y el privado, entidades del sector privado han adoptado criterios proactivos para investigar operaciones de la delincuencia cibernética e interponer acciones judiciales. Esas acciones complementan las de las fuerzas del orden y pueden ayudar a mitigar los daños ocasionados a las víctimas. Las instituciones académicas desempeñan diversos papeles en la prevención del delito cibernético, por ejemplo con la instrucción y capacitación de profesionales, la elaboración de normas y la formulación de políticas, así como su labor en la elaboración de normas técnicas y formulación de soluciones. En las universidades se congregan expertos en delitos cibernéticos, algunos equipos de respuesta a emergencias informáticas y centros de investigación especializada y se facilitan sus respectivas labores.

## B. Resumen de las principales conclusiones del estudio

51. Las principales conclusiones del estudio exhaustivo sobre el delito cibernético son las siguientes:

a) La fragmentación a nivel internacional y la diversidad en las leyes nacionales sobre delitos cibernéticos pueden tener relación con la existencia de múltiples instrumentos de diferente alcance temático y geográfico. Si bien es legítimo que los instrumentos reflejen diferencias socioculturales y regionales, las discrepancias en cuanto al alcance de la competencia procesal y de las disposiciones internacionales de cooperación pueden llevar a la aparición de “grupos” de países a efectos de cooperación que no siempre son convenientes para el carácter mundial del delito cibernético;

b) La dependencia de formas tradicionales de cooperación internacional oficial en los asuntos relativos al delito cibernético no puede ofrecer actualmente la respuesta oportuna necesaria para obtener las volátiles pruebas electrónicas. Como un creciente número de delitos implican pruebas electrónicas repartidas por el mundo, esto será un problema no solo para el delito cibernético sino para todos los delitos en general;

c) En un mundo de computación en la nube y de centros de datos, habrá que replantearse el papel de la “ubicación” de las pruebas, incluida la posibilidad de obtener consenso sobre cuestiones relativas al acceso directo de las fuerzas del orden a los datos extraterritoriales;

d) El análisis de los marcos jurídicos nacionales disponibles indica una armonización insuficiente de los delitos cibernéticos “primordiales”, de las facultades investigativas y de la admisibilidad de las pruebas electrónicas. Las

normas internacionales de derechos humanos representan un importante punto de referencia externa para la tipificación como delito y para las disposiciones procesales;

e) Las fuerzas del orden, los fiscales y los jueces de los países en desarrollo necesitan ayuda y asistencia técnicas de largo plazo, sostenibles y amplias para investigar y combatir el delito cibernético;

f) Las actividades de prevención del delito cibernético en todos los países deben consolidarse con un enfoque integral que implique una mayor sensibilización, alianzas entre los sectores público y privado y la integración de las estrategias de lucha contra el delito cibernético en una perspectiva más amplia de la seguridad cibernética.

## C. Resumen de las opciones que figuran en el estudio

52. Las opciones recogidas en el estudio elaborado por la UNODC se configuraron a partir de las respuestas de los países a una pregunta en el cuestionario del estudio acerca de las opciones que se podrían examinar para fortalecer las actuales respuestas jurídicas o de otra índole ante el delito cibernético en los planos nacional e internacional y proponer otras nuevas, y a partir también de las conclusiones principales. En el estudio se determina que entre esas opciones pueden figurar una o más de las siguientes[9]:

a) la elaboración de disposiciones internacionales modelo sobre la tipificación como delito de los actos delictivos cibernéticos primordiales a fin de ayudar a los Estados a eliminar los refugios seguros mediante la adopción de elementos de los delitos comunes;

b) la elaboración de disposiciones internacionales modelo sobre las facultades para investigar las pruebas electrónicas con miras a ayudar a los Estados a establecer los mecanismos procesales necesarios para investigar delitos que impliquen pruebas electrónicas;

c) la elaboración de disposiciones modelo sobre jurisdicción a fin de establecer al respecto bases comunes efectivas de atribución de la jurisdicción en asuntos penales relacionados con el delito cibernético;

d) la elaboración de disposiciones modelo sobre cooperación internacional en el caso de las pruebas electrónicas para su inclusión en instrumentos bilaterales o multilaterales, por ejemplo en un texto revisado del Tratado modelo de asistencia recíproca en asuntos penales, en concordancia con las sugerencias contenidas en la guía para las deliberaciones del 13° Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal;

e) la elaboración de un instrumento multilateral sobre la cooperación internacional respecto de las pruebas electrónicas en los asuntos penales, a fin de contar con un mecanismo internacional de cooperación para la conservación y obtención de pruebas electrónicas;

---

[9] Para más detalles, véase UNODC/CCPCJ/EG.4/2013/2.

f) la elaboración de un instrumento multilateral amplio sobre el delito cibernético con el objeto de fijar un criterio internacional en materia de tipificación, competencia procesal, jurisdicción y cooperación internacional;

g) la consolidación de las alianzas internacionales, regionales y nacionales, incluidas las alianzas con el sector privado y con instituciones académicas, a fin prestar una mejor asistencia técnica para la prevención y represión del delito cibernético en los países en desarrollo.

# V. Recomendaciones destinadas a la promoción de las actividades relativas a la lucha contra el delito cibernético, incluidos la asistencia técnica y el fomento de la capacidad

53. La Comisión tal vez desee solicitar a la UNODC que, sobre la base, entre otras cosas, de sus actividades reseñadas en la sección II del presente informe, siga prestando asistencia técnica a los Estados Miembros para hacer frente al delito cibernético y exhorte a los Estados Miembros a que aporten para ello recursos extrapresupuestarios a fin de asegurar el fomento de la capacidad sostenible a largo plazo de los países en desarrollo en la lucha contra el delito cibernético.