



12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal



Salvador (Brasil), 12 a 19 de abril de 2010

Distr. general
22 de enero de 2010
Español
Original: inglés

Tema 8 del programa provisional*

Novedades recientes en el uso de la ciencia y la tecnología por los delincuentes y por las autoridades competentes en la lucha contra la delincuencia, incluido el delito cibernético

Novedades recientes en el uso de la ciencia y la tecnología por los delincuentes y por las autoridades competentes en la lucha contra la delincuencia, incluido el delito cibernético

Documento de trabajo preparado por la Secretaría

I. Introducción

1. El hecho de que el delito cibernético ocupe un lugar destacado en el programa del 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal pone de relieve la gran importancia que sigue teniendo este tema y los serios retos que plantea, a pesar de los debates que se vienen sosteniendo al respecto desde hace casi medio siglo.
2. En los últimos 50 años se han examinado y elaborado diversas soluciones para hacer frente a la cuestión del delito cibernético. En parte, el tema sigue siendo problemático porque la tecnología evoluciona constantemente y los métodos utilizados para cometer esos delitos también cambian.
3. Desde el decenio de 1960 hasta el de 1980, los Estados tuvieron que hacer frente a nuevos actos, tales como la manipulación informática y el espionaje de datos, para los que no había legislación penal. En esos años, el debate se centró en la elaboración de una respuesta jurídica¹.

* A/CONF.213/1.

¹ Véase Susan H. Nycum, *The Criminal Law Aspects of Computer Abuse: Applicability of the State Penal Laws to Computer Abuse* (Menlo Park, California, Stanford Research Institute, 1976) y Ulrich Sieber, *Computerkriminalität und Strafrecht* (Colonia, Karl Heymanns Verlag, 1977).



4. La introducción de la interfaz gráfica en los años noventa, a la que siguió un rápido aumento del número de usuarios de Internet, engendró nuevos desafíos. La información colocada legalmente en Internet en un país pasó a estar disponible en todo el mundo, incluso en aquellos países en que su publicación no era legal. Otro aspecto preocupante de los servicios en línea fue la rapidez del intercambio de información, que resultó ser especialmente problemática para la investigación de los delitos con dimensiones transnacionales².
5. En el primer decenio del siglo XXI han predominado los métodos nuevos y sofisticados para delinquir (tales como la “pesca de datos” o “phishing”³ y los ataques con redes zombi o “botnets”⁴) y el uso de tecnologías que resultan aún más difíciles de controlar para los funcionarios encargados de las investigaciones (tales como las comunicaciones con transmisión de voz sobre Protocolo de Internet (VoIP) y la informática en nube (“cloud computing”).

II. Los retos del delito cibernético

A. La incertidumbre del alcance

6. A pesar de las mejoras tecnológicas y de las intensas investigaciones realizadas, el grado en que la tecnología de la información se utiliza para fines ilegales se mantiene estable o tal vez esté incluso aumentando. Algunos proveedores de servicios de correo electrónico han notificado que entre el 75% y el 90% de todos los mensajes son correos basura⁵. También se han comunicado cifras constantes o crecientes respecto de otras conductas delictivas más generalizadas. Por ejemplo, la Internet Watch Foundation, en su Annual and Charity Report de 2008, informó de que el número de sitios web comerciales de pornografía infantil se había mantenido bastante estable entre 2006 y 2008.
7. Si bien la información estadística es útil para poner de relieve la importancia constante o creciente de la cuestión, uno de los principales retos relacionados con el delito cibernético es la falta de información fidedigna sobre el alcance del problema y sobre las detenciones, los enjuiciamientos y las condenas correspondientes.

² En lo que respecta a las formas en que la mayor rapidez del intercambio de datos ha repercutido en las investigaciones de los delitos cibernéticos, véase Unión Internacional de Telecomunicaciones, *El ciberdelito: Guía para los países en desarrollo* (Ginebra, 2009). Disponible en http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf.

³ Según lo describe la Unión Internacional de Telecomunicaciones en *El ciberdelito: Guía* (véase la nota de pie de página 2), el “phishing” es un acto que tiene por objeto lograr que la víctima revele información personal o confidencial. El término “phishing” se empleó inicialmente para describir la utilización de los correos electrónicos para “pescar” (en inglés, “phish”) contraseñas y datos financieros en un mar de usuarios de Internet. El empleo de la grafía “ph” se relaciona con las convenciones terminológicas de uso común en la piratería informática.

⁴ Una red zombi o “botnet” es un grupo de computadoras afectadas en que se ejecuta un programa informático bajo control externo. Véase Clay Wilson, “Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress”, Congressional Research Service Report RL32114, actualizado el 29 de enero de 2008, disponible en <http://www.fas.org/sgp/crs/terror/RL32114.pdf>.

⁵ El Grupo de Trabajo contra el uso indebido de los mensajes comunicó en 2009 que entre el 85% y el 90% de todos los correos electrónicos eran correos basura (http://www.maawg.org/sites/maawg/files/news/2009_MAAWG-Consumer_Survey-Part1.pdf).

Las estadísticas relativas a la delincuencia no suelen mencionar los delitos por separado, y las pocas estadísticas que existen sobre el impacto del delito cibernético no son, por lo general, lo suficientemente detalladas como para proporcionar a los responsables de la formulación de políticas información fidedigna sobre la escala o el alcance de los delitos⁶. Sin esos datos, es difícil cuantificar el impacto del delito cibernético en la sociedad y elaborar estrategias para combatirlo⁷.

8. Uno de los motivos por los que falta información estadística es que no es fácil estimar el alcance de la pérdida financiera y el número de delitos cometidos por los delincuentes cibernéticos. Según algunas fuentes, las pérdidas que sufren anualmente las empresas e instituciones de los Estados Unidos⁸ a causa del delito cibernético se cifran en 67.000 millones de dólares de los EE.UU.; sin embargo, no es seguro que la extrapolación de los resultados obtenidos en estudios por muestreo esté justificada⁹. Esta crítica metodológica se aplica no sólo a las pérdidas, sino también al número de delitos reconocidos¹⁰. Tampoco se sabe con seguridad en qué medida las víctimas informan sobre los delitos cibernéticos. Aunque las autoridades que combaten estos delitos alientan a las víctimas a que notifiquen los casos, se teme que, en particular en el sector financiero, las víctimas (por ejemplo, los bancos) no informen de los casos por miedo a que la publicidad negativa dañe su reputación¹¹. Si una empresa anuncia que su servidor ha sido objeto de actos de piratería informática, los clientes pueden perder la confianza, y el costo y las consecuencias totales para la empresa podrían ser aún mayores que las pérdidas causadas por el ataque de piratería. Además, las víctimas pueden no confiar en que los organismos represión sean capaces de identificar a los delincuentes. Sin embargo, si los delitos no se notifican y no se enjuicia a los delincuentes, éstos volverán probablemente a delinquir.

9. Otra dificultad relacionada con la información estadística es que con mucha frecuencia se cita repetidamente información que no es fidedigna ni verificable. Un ejemplo de ello es la información estadística sobre los aspectos comerciales de la pornografía infantil en Internet. En varios análisis se ha citado que la pornografía infantil en Internet genera 2.500 millones de dólares anuales a nivel mundial¹². Sin embargo, la fuente de esa cifra (www.toptenreviews.com) no proporciona ningún antecedente sobre la manera en que se realizó la investigación. Dado que la empresa, en su sitio web, afirma que “le ofrece la información que usted necesita para hacer una compra atinada; le recomienda el mejor producto de cada categoría y,

⁶ Estados Unidos de América, Oficina General de Contabilidad, *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats*, informe de la Oficina General de Contabilidad GAO-07-705 (Washington, D.C., junio de 2007), pág. 22; e Ian Walden, *Computer Crimes and Digital Investigations* (Oxford, Oxford University Press, 2007).

⁷ Walden, *Computer Crimes and Digital Investigations*.

⁸ Estados Unidos, Oficina Federal de Investigación, *2005 FBI Computer Crime Survey*, pág. 10.

⁹ *El cibercriminólogo: Guía* (véase la nota de pie de página 2).

¹⁰ *Ibid.*

¹¹ Neil Mitchison y Robin Urry, “Crime and abuse in e-business”. *IPTS Report*, vol. 57, septiembre de 2001.

¹² Kim-Kwang Choo, Russel G. Smith y Rob McCusker, “Future directions in technology-enabled crime: 2007-09”, *Research and Public Policy Series*, Núm. 78 (Canberra, Instituto Australiano de Criminología, 2007), pág. 62; ECPAT International, *Violence against Children in Cyberspace* (Bangkok, 2005), pág. 54; Consejo de Europa, *Organised Crime Situation Report 2005: Focus on the Threat to Economic Crime* (Estrasburgo, diciembre de 2005), pág. 41.

con sus gráficos de comparación directa, noticias, artículos y vídeos, simplifica el proceso de compra del consumidor”, cabe dudar seriamente de la fiabilidad de los datos. Otro ejemplo: en 2006, un periodista de *The Wall Street Journal*¹³ que investigaba la afirmación de que la pornografía infantil era un negocio de 20.000 millones de dólares anuales, descubrió que los dos documentos principales que daban información sobre los ingresos, con cifras que iban de 3.000 millones a 20.000 millones (publicaciones del National Center for Missing and Exploited Children, en los Estados Unidos, y del Consejo de Europa), remitían a instituciones que no confirmaron las cifras.

B. La dimensión transnacional

10. El delito cibernético es en gran medida un delito de carácter transnacional. Internet se concibió inicialmente como una red militar basada en una arquitectura de red descentralizada. Debido a esta estructura básica y a la disponibilidad mundial de los servicios, el delito cibernético suele tener una dimensión internacional. Es fácil enviar correos electrónicos con un contenido ilegal a destinatarios de una serie de países, incluso cuando el remitente inicial y el destinatario final se encuentran en el mismo país o cuando ya sea el remitente o el destinatario utilizan un servicio de correo electrónico prestado por un proveedor situado fuera del país. Algunos de los proveedores de servicios gratuitos de correo electrónico más conocidos tienen millones de usuarios en todo el mundo, lo que refuerza la dimensión transnacional del delito cibernético.

11. Las dificultades que el elemento transnacional plantea para la investigación del delito cibernético son parecidas a las que entrañan otros delitos transnacionales. Como consecuencia del principio fundamental de la soberanía nacional, según el cual no pueden realizarse investigaciones en territorios extranjeros sin el permiso de las autoridades locales, la cooperación estrecha entre los Estados involucrados es crucial para la investigación de los delitos cibernéticos. Otra dificultad importante se relaciona con el poco tiempo disponible para llevar a cabo las investigaciones de esos delitos. A diferencia de lo que ocurre con las drogas ilícitas, que, según el medio de transporte que se utilice, pueden tardar semanas en llegar a su destino, los correos electrónicos se envían en segundos y, si se tiene acceso a un ancho de banda adecuado, es posible descargar grandes ficheros en algunos minutos.

12. La cooperación tempestiva y eficaz entre las autoridades de diferentes países es fundamental también porque en los casos de delitos cibernéticos las pruebas suelen suprimirse automáticamente y al cabo de poco tiempo. Los procedimientos oficiales prolongados pueden obstaculizar seriamente las investigaciones.

13. Muchos de los acuerdos de asistencia judicial recíproca existentes aún se basan en procedimientos oficiales, complejos y a menudo prolongados. Por consiguiente, el establecimiento de procedimientos para responder rápidamente a los incidentes y a las solicitudes de cooperación internacional se considera de importancia vital.

¹³ Carl Bialik, “Measuring the child-porn trade”, *The Wall Street Journal*, 18 de abril de 2006.

14. En el capítulo III del Convenio sobre la Ciberdelincuencia, del Consejo de Europa¹⁴, figura un conjunto de principios para la elaboración de un régimen jurídico de cooperación internacional en las investigaciones sobre delitos cibernéticos. En ese capítulo se examina la importancia creciente de la cooperación internacional (artículos 23 a 35) y se promueve el uso de medios de comunicación expeditos, como el fax y el correo electrónico (artículo 25, párrafo 3). Además, se insta a las Partes en el Convenio a que designen un punto de contacto disponible las 24 horas del día, todos los días de la semana, para responder a las solicitudes de asistencia de los Estados (artículo 35). Otros criterios a este respecto figuran en el proyecto de convención internacional para aumentar la protección contra el delito cibernético y el terrorismo, así como en el proyecto de manual de la Unión Internacional de Telecomunicaciones (UIT) sobre la legislación contra el delito cibernético.

C. Las diferencias en los enfoques jurídicos nacionales

15. Un efecto práctico de la arquitectura en red de Internet es que los autores de los delitos cibernéticos no necesitan estar presentes en el lugar del delito. Por ello, impedir la existencia de refugios seguros para los delincuentes se ha convertido en un aspecto clave de la prevención del delito cibernético¹⁵. Los delincuentes utilizarán refugios seguros para obstaculizar las investigaciones. Un ejemplo bien conocido es el gusano informático “Love Bug”, desarrollado en Filipinas en 2000¹⁶, que al parecer infectó a millones de computadoras en todo el mundo¹⁷. Las investigaciones locales se vieron impedidas por el hecho de que, en esa época, el desarrollo y la difusión intencionales del programa informático dañino no estaban debidamente penalizados en Filipinas.

16. La cuestión de la convergencia de la legislación es sumamente pertinente, puesto que un gran número de países fundamenta su régimen de asistencia judicial recíproca en el principio de la doble incriminación, según el cual un delito debe ser considerado como tal tanto en el Estado que solicita la asistencia como en el que la

¹⁴ Consejo de Europa, *European Treaty Series*, No. 185. Véase también el “informe explicativo” de ese Convenio.

¹⁵ Tanto la Asamblea General, en su resolución 55/63, como el Grupo de los Ocho, en los principios y el plan de acción para combatir la delincuencia de alta tecnología aprobados en la Reunión de Ministros de Justicia y del Interior del Grupo de los Ocho celebrada en Washington, D.C., el 10 de diciembre de 1997 (disponible en www.justice.gov/criminal/cybercrime/g82004/97Communique.pdf), han destacado la necesidad de eliminar los refugios seguros para quienes utilicen indebidamente, con fines delictivos, las tecnologías de la información.

¹⁶ Estados Unidos, Oficina General de Contabilidad, *Critical Infrastructure Protection: “ILOVEYOU” Computer Virus Highlights Need for Improved Alert and Coordination Capabilities*, testimonio prestado ante el Subcomité de Instituciones Financieras, Comité de Asuntos Bancarios, Urbanos y de la Vivienda, Senado de los Estados Unidos, informe de la Oficina General de Contabilidad GAO/T-AIMD-00-181 (Washington, D.C., mayo de 2000).

¹⁷ “Police close in on Love Bug culprit”, BBC News, 6 de mayo de 2000. Disponible en <http://news.bbc.co.uk/2/hi/science/nature/738537.stm>.

presta¹⁸. Las investigaciones a nivel mundial se limitan, por lo general, a los actos que están tipificados como delito en todos los países afectados. Aunque existe una serie de delitos que pueden ser perseguidos en cualquier parte del mundo, las diferencias regionales desempeñan un papel importante. Por ejemplo, en diferentes países se penalizan diferentes tipos de contenidos¹⁹, lo que significa que el material que se coloca legalmente en un servidor en un país puede ser considerado ilegal en otro²⁰.

17. La tecnología informática y de red que se utiliza en la actualidad es básicamente la misma en todo el mundo. Aparte de las cuestiones del idioma y de los adaptadores de corriente, hay muy poca diferencia entre los sistemas informáticos y los teléfonos móviles que se venden en Asia y en Europa. En relación con Internet la situación es análoga. Debido a la normalización, los protocolos utilizados en países de África son los mismos que los que se emplean en los Estados Unidos. La normalización permite a los usuarios de todo el mundo acceder a los mismos servicios a través de Internet²¹.

18. En los párrafos que siguen se examinan dos criterios diferentes para hacer frente a la dimensión transnacional del delito cibernético y a las diferencias en las normas jurídicas.

1. Compatibilidad de la legislación

19. Una forma de abordar la dimensión transnacional del delito cibernético y mejorar la cooperación internacional es desarrollar y normalizar la legislación pertinente. En los últimos años se han adoptado varias iniciativas regionales.

20. En 2002, el Commonwealth elaboró una ley modelo sobre el delito cibernético e informático con la finalidad de mejorar la legislación para combatir la ciberdelincuencia en los Estados miembros del Commonwealth e intensificar la cooperación internacional. Sin esas mejoras, se necesitarían por lo menos 1.272 tratados bilaterales entre los Estados del Commonwealth para que los países

¹⁸ En lo que respecta al principio de la doble incriminación en las investigaciones de delitos cibernéticos, véanse el Manual de las Naciones Unidas sobre Prevención y Control de Delitos Informáticos (Revista Internacional de Política Criminal, Núms. 43 y 44: publicación de las Naciones Unidas, Núm. de venta S.94.IV.5), pág. 269, y el documento de antecedentes de Stein Schjøberg y Amanda Hubbard titulado “Harmonizing national legal approaches on cybercrime”, pág. 5, que se presentó en la Reunión temática de la UIT sobre seguridad cibernética celebrada en Ginebra del 28 de junio al 1° de julio de 2005.

¹⁹ Los diferentes enfoques jurídicos que regulan el contenido son uno de los motivos por los que ciertos aspectos del contenido ilegal no están incluidos en el Convenio sobre la Ciberdelincuencia sino que se tratan en un protocolo adicional. Véase también *El ciberdelito: Guía*, cap. 2.5 (véase la nota de pie de página 2).

²⁰ En lo que respecta a los diferentes criterios nacionales relativos a la penalización de la pornografía infantil, véase, por ejemplo, Ulrich Sieber, *Kinderpornographie, Jugendschutz und Providerverantwortlichkeit im Internet: eine strafrechtsvergleichende Untersuchung* (Bonn, Forum Verlag Godesberg, 1999).

²¹ En lo que respecta a la importancia de la uniformidad de las normas técnicas y las normas jurídicas, véase Marco Gercke, “National, regional and international approaches in the fight against cybercrime”, *Computer Law Review International*, 2008, pág. 7.

podieran cooperar entre sí en esta materia²². La ley modelo contiene disposiciones sobre el derecho penal sustantivo, el derecho procesal y la cooperación internacional. Debido al enfoque regional de la ley modelo, el efecto en la armonización se limita a los Estados miembros del Commonwealth.

21. La Unión Europea también ha hecho esfuerzos por armonizar la legislación sobre el delito cibernético entre sus 27 Estados miembros, por ejemplo mediante lo siguiente: la directiva 2000/31/EC del Parlamento Europeo y el Consejo sobre ciertos aspectos jurídicos de los servicios en la sociedad de la información, en particular el comercio electrónico, en el mercado interno; la decisión marco 2000/413/JHA del Consejo de la Unión Europea sobre la lucha contra el fraude y la falsificación de medios de pago distintos del efectivo; la decisión marco 2004/68/JHA del Consejo de la Unión Europea sobre la lucha contra la explotación sexual de los niños y la pornografía infantil; la decisión marco 2005/222/JHA del Consejo de la Unión Europea sobre los ataques contra los sistemas de información²³; la directiva 2006/24/EC del Parlamento Europeo y del Consejo de la Unión Europea sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas de acceso público o de redes públicas de comunicaciones y por la que se modificó la directiva 2002/58/EC; y la decisión marco 2008/919/JHA del Consejo de la Unión Europea por la que se modificó la decisión marco 2002/475/JHA sobre la lucha contra el terrorismo. A diferencia de lo que ocurre en la mayoría de los otros enfoques regionales, la aplicación de los instrumentos adoptados por la Unión Europea es obligatoria para todos los Estados miembros. Si bien los instrumentos son efectivos, el principal obstáculo a la armonización dentro de la Unión Europea era, al menos hasta comienzos de 2010, el limitado poder de la legislación en la esfera del derecho penal²⁴. La diversidad de enfoques obedecía a que la capacidad de la Unión Europea de armonizar el derecho penal nacional se limitaba a algunas esferas especiales²⁵. El Tratado de Lisboa, por el que se modificó el Tratado de la Unión Europea y el Tratado constitutivo de la Comunidad Europea, ha cambiado la situación y confiere a la Unión Europea mayores atribuciones para armonizar la legislación sobre el delito informático en el futuro; ello, sin embargo, se limita a los 27 Estados miembros.

22. El Consejo de Europa ha elaborado tres instrumentos principales para armonizar la legislación sobre el delito cibernético. El más conocido es el Convenio sobre la Ciberdelincuencia, redactado entre 1997 y 2001. Este Convenio contiene

²² Richard Bourne, “2002 Commonwealth Law Ministers’ Meeting: policy brief”, preparado para la Reunión de Ministros de Justicia del Commonwealth, celebrada en Kingstown (San Vicente y las Granadinas) del 18 al 21 de noviembre de 2002 (Londres, Institute of Commonwealth Studies, 2002), pág. 9.

²³ Para obtener más información, véanse Marco Gercke, “The EU framework decision on attacks against information systems”, *Computer und Recht*, 2005, págs. 468 y ss.; y *El ciberdelito: Guía* (véase la nota de pie de página 2), pág. 107.

²⁴ Helmut Satzger, *Internationales und Europäisches Strafrecht* (Baden-Baden, Nomos, 2005), pág. 84; y P.J.G. Kapteyn y Pieter Verloren van Themaat, *Introduction to the Law of the European Communities: After the Coming into Force of the Single European Act* (Boston, Kluwer Law International, 1989).

²⁵ En lo que respecta a la legislación sobre el delito cibernético en los países de la Unión Europea, véase Lorenzo Valeri y otros, *Handbook of Legal Procedures of Computer Network Misuse in EU Countries* (Santa Monica, California, Rand Corporation, 2006).

disposiciones sobre el derecho penal sustantivo, el derecho procesal y la cooperación internacional. Al mes de diciembre de 2009 había sido firmado por 46 Estados y ratificado por 26. Puesto que, durante la negociación del Convenio, no fue posible llegar a un acuerdo sobre la penalización del racismo y la distribución de material xenófobo, en 2003 se estableció el Protocolo Adicional del Convenio sobre la Ciberdelincuencia, relativo a la penalización de los actos de naturaleza racista y xenófoba cometidos por medio de sistemas informáticos²⁶. Al mes de diciembre de 2009, 34 Estados²⁷ habían firmado el Protocolo Adicional, y 15 de ellos²⁸ lo habían ratificado. En 2007 se abrió a la firma el Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual²⁹. Este Convenio contiene disposiciones específicas que penalizan el intercambio de pornografía infantil así como la obtención, a sabiendas, de acceso a pornografía infantil a través de las tecnologías de la información y las comunicaciones (párrafo 1 f) del artículo 20). Al mes de diciembre de 2009 habían firmado este Convenio 38 Estados³⁰, y tres de ellos³¹ lo habían ratificado.

23. Además, cabe mencionar el proyecto de convención internacional para mejorar la protección contra el delito cibernético y el terrorismo, elaborado como medida de seguimiento de una conferencia acogida por la Universidad de Stanford (Estados Unidos) en 1999, y el proyecto de manual de la UIT sobre la legislación contra el delito cibernético, elaborado por representantes de la American Bar Association y otros expertos.

2. Territorialización

24. Teóricamente, los cambios dimanantes de la normalización técnica van mucho más allá de la globalización de la tecnología y los servicios y podrían conducir a la armonización de las legislaciones nacionales. Sin embargo, como lo indican la situación de la ratificación del Convenio sobre la Ciberdelincuencia y la negociación del Protocolo Adicional del Convenio, los principios de la legislación nacional cambian con mucha mayor lentitud que los aspectos técnicos. A ello obedece la segunda iniciativa: los enfoques encaminados a territorializar Internet.

²⁶ Consejo de Europa, *European Treaty Series*, Núm. 189. Véase también el “informe explicativo” del Protocolo Adicional.

²⁷ Albania, Alemania, Armenia, Austria, Bélgica, Bosnia y Herzegovina, Canadá, Chipre, Croacia, Dinamarca, Eslovenia, Estonia, la ex República Yugoslava de Macedonia, Finlandia, Francia, Grecia, Islandia, Letonia, Liechtenstein, Lituania, Luxemburgo, Malta, Montenegro, Noruega, Países Bajos, Polonia, Portugal, República de Moldova, Rumania, Serbia, Sudáfrica, Suecia, Suiza y Ucrania.

²⁸ Albania, Armenia, Bosnia y Herzegovina, Chipre, Croacia, Dinamarca, Eslovenia, la ex República Yugoslava de Macedonia, Francia, Letonia, Lituania, Noruega, Rumania, Serbia y Ucrania.

²⁹ Consejo de Europa, *Treaty Series*, Núm. 201.

³⁰ Albania, Alemania, Austria, Azerbaiyán, Bélgica, Bulgaria, Chipre, Croacia, Dinamarca, Eslovaquia, Eslovenia, España, Estonia, la ex República Yugoslava de Macedonia, Finlandia, Francia, Georgia, Grecia, Irlanda, Islandia, Italia, Liechtenstein, Lituania, Luxemburgo, Mónaco, Montenegro, Noruega, Países Bajos, Polonia, Portugal, República de Moldova, Reino Unido, Rumania, San Marino, Serbia, Suecia, Turquía y Ucrania.

³¹ Albania, Dinamarca y Grecia.

25. Aunque Internet pueda estar al margen de los controles fronterizos, hay formas de restringir el acceso a determinada información³². En vista de ello, los gobiernos nacionales y las organizaciones internacionales han comenzado a prestar atención a las obligaciones de los proveedores de servicios de Internet de bloquear el acceso a los sitios web que contengan pornografía infantil³³. Desde el punto de vista técnico, los proveedores de acceso pueden en general controlar si el sitio web al que el usuario desea entrar está en una lista negra y bloquear esa entrada. Las soluciones técnicas van desde la manipulación del sistema de nombres de dominio y el uso de servidores intermediarios hasta soluciones híbridas que combinan diversos métodos³⁴. La Iniciativa OpenNet informa de que ese tipo de control del contenido se practica en unos 25 países aproximadamente³⁵. Varios países europeos, entre ellos Italia, Noruega, el Reino Unido, Suecia y Suiza, y países tales como China, el Irán (República Islámica del) y Tailandia utilizan este método. La Unión Europea también está examinando la posibilidad de imponer esas obligaciones³⁶. Las preocupaciones en relación con este método giran en torno al hecho de que todas las soluciones técnicas actualmente disponibles pueden soslayarse, y existe también el riesgo de actuar con exceso de celo al bloquear el acceso a la información de Internet³⁷. La importancia de proteger los derechos fundamentales ha sido señalada por el Consejo de Europa en la recomendación de su Comité de Ministros sobre las

³² Jonathan Zittrain, "A history of online gatekeeping", *Harvard Journal of Law and Technology*, vol. 19, Núm. 2 (2006), pág. 253.

³³ Con respecto a las obligaciones y los enfoques relativos a los filtros, véanse Ilaria Lonardo, "Italy: Service Provider's Duty to Block Content", *Computer Law Review International*, 2007, págs. 89 y ss.; Ulrich Sieber y Malaika Nolde, *Sperrverfügungen im Internet: Nationale Rechtdurchsetzung im globalen Cyberspace?* (Berlín, Duncker & Humblot, 2008); W. Ph. Stol y otros, *Filteren van kinderporno op internet: Een verkenning van technieken en reguleringen in binnen- en buitenland* (La Haya, Boom Juridische Uitgevers, WODC, 2008); Tom Edwards y Gareth Griffith, "Internet censorship and mandatory filtering", *NSW Parliamentary Library Research Service*, E-Brief 5/08, noviembre de 2008; Jonathan Zittrain y Benjamin Edelman, "Documentation of Internet filtering worldwide", octubre de 2003, proyecto disponible en <http://cyber.law.harvard.edu/filtering>.

³⁴ Para una reseña general de los aspectos técnicos, véanse Sieber y Nolde, *Sperrverfügungen im Internet*, págs. 50 y ss.; Stol y otros, *Filteren van kinderporno op internet*, págs. 10 y ss.; Andreas Pfitzmann, Stefan Köpsell y Thomas Kriegelstein, *Sperrverfügungen gegen Access-Provider: Technisches Gutachten*, Universidad Técnica de Dresden, disponible en www.eco.de/dokumente/20080428_technisches_Gutachten_Sperrveruegungen.pdf; Richard Clayton, Steven J. Murdoch y Robert N. M. Watson, "Ignoring the Great Firewall of China", documento presentado en el Sexto curso práctico sobre tecnologías que aumentan la privacidad, Cambridge, junio de 2006; Lori Brown Ayre, *Internet Filtering Options Analysis: An Interim Report, preparado para el proyecto InfoPeople*, mayo de 2001.

³⁵ Miklós Haraszti, "Preface", en *Governing the Internet: Freedom and Regulation in the OSCE Region*, C. Möller y A. Amouroux, eds. (Viena, Organización para la Seguridad y la Cooperación en Europa, 2007), págs. 5 y 6.

³⁶ Comisión de las Comunidades Europeas, "Proposal for a Council framework decision on combating the sexual abuse, sexual exploitation of children and child pornography, repealing framework decision 2004/68/JHA", documento COM(2009) 135, Bruselas, 25 de marzo de 2009.

³⁷ Para obtener más información sobre el bloqueo de Internet y el equilibrio entre las libertades fundamentales, véase Cormac Callanan y otros, *Internet Blocking: Balancing Cybercrime Responses in Democratic Societies* (Dublín, Aconite Internet Solutions, octubre de 2009), caps. 6 y 7.

medidas para promover el respeto de la libertad de expresión e información con respecto a los filtros en Internet.

D. La delincuencia organizada

26. Si bien los delitos informáticos son obra, por lo general, de personas aisladas, también intervienen en ellos grupos delictivos organizados. Este elemento es especialmente importante, porque abre la posibilidad de aplicar instrumentos concebidos para combatir la delincuencia organizada, como la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional³⁸.

27. Al examinar el tema del delito cibernético y la delincuencia organizada, es necesario distinguir entre dos categorías principales de actuación de los grupos delictivos: la utilización de la tecnología de la información por los grupos delictivos organizados tradicionales, y la comisión de delitos cibernéticos por grupos delictivos organizados³⁹.

28. Los grupos delictivos organizados tradicionales que no tienen antecedentes de actividades delictivas relacionadas con Internet están utilizando la tecnología de la información para coordinar sus actividades y aumentar su eficacia en la comisión de delitos⁴⁰. En estos casos, la tecnología de la información se utiliza para mejorar la eficiencia del grupo delictivo organizado en su campo de actividad tradicional. Ello incluye la utilización de las comunicaciones electrónicas, que le permiten, por ejemplo, hacer uso de la tecnología de cifrado y comunicar en forma anónima. Además, Internet puede servir para ampliar los mercados ya que, como ha descubierto el Grupo de Tareas sobre la Delincuencia Organizada del Reino Unido, Internet ha abierto un mercado nuevo y mucho mayor para quienes venden productos falsificados y pirateados⁴¹.

29. Los informes indican que los grupos delictivos organizados tradicionales están tendiendo a emprender nuevas formas de actividades delictivas en la esfera de los delitos de alta tecnología⁴². Ello incluye la piratería de programas informáticos y otras formas de violación de los derechos de autor⁴³. Pero también otras esferas del

³⁸ Naciones Unidas, *Treaty Series*, vol. 2225, Núm. 39574.

³⁹ Kim-Kwang Raymond Choo, "Organised crime groups in cyberspace: a typology", *Trends in Organized Crime*, vol. 11, Núm. 3 (septiembre de 2008), págs. 270 a 295. En este artículo, Choo sugiere que hay tres categorías de grupos delictivos organizados que explotan las tecnologías de la información para infringir los controles.

⁴⁰ *Ibid.*, pág. 273; Eoghan Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*, 2ª ed. (Londres, Academic Press, 2004), pág. 9.

⁴¹ Reino Unido, Grupo de Tareas sobre la Delincuencia Organizada, *Annual Report and Threat Assessment 2007: Organised Crime in Northern Ireland (2007)*, pág. 34. Disponible en www.octf.gov.uk.

⁴² Reino Unido, Organismo contra la Delincuencia Organizada Grave, *The United Kingdom Threat Assessment of Organised Crime: 2009/10*, pág. 10. Disponible en www.soca.gov.uk.

⁴³ Canadá, Servicio de Inteligencia y Seguridad del Canadá, "Transnational criminal activity: a global context", *Perspectives*, 17 de agosto de 2000, disponible en www.csis-scrs.gc.ca/pblctns/prspctvs/200007-eng.asp; Choo, "Organised crime groups", pág. 273 (véase la nota de pie de página 40).

delito cibernético, como la pornografía infantil⁴⁴ y los delitos relacionados con la identidad, están vinculados a menudo con la delincuencia organizada. En lo que respecta a la aplicación de la Convención contra la Delincuencia Organizada, deben tenerse en cuenta las siguientes características especiales de los grupos organizados que cometen delitos cibernéticos:

- a) Los grupos dedicados al delito cibernético suelen tener una estructura más flexible y abierta, que permite la incorporación de nuevos miembros por un período de tiempo limitado⁴⁵;
- b) Los grupos que cometen delitos cibernéticos son con frecuencia mucho más pequeños que los grupos delictivos organizados tradicionales⁴⁶;
- c) En muchos casos, los miembros de los grupos comunican entre sí exclusivamente en forma electrónica, sin tener nunca encuentros personales.

III. Respuesta al delito cibernético

30. Las organizaciones internacionales y regionales, los gobiernos nacionales, los organismos encargados de hacer cumplir la ley y las organizaciones no gubernamentales están abordando el delito cibernético de diferentes formas, que incluyen medios legislativos, de aplicación de la ley y de fomento de la capacidad.

A. Legislación

31. Actualmente, la elaboración de leyes sobre el delito cibernético tiene lugar principalmente a nivel nacional y regional. A diferencia de lo que ocurre con las normas técnicas utilizadas en los procesos de transferencia de datos, que son las mismas en todas partes del mundo, hasta la fecha no se ha hecho nada para armonizar la legislación sobre el delito cibernético a nivel mundial.

1. El limitado alcance de los instrumentos ya existentes

32. La repercusión mundial de los enfoques regionales adoptados por el Commonwealth, la Comunidad Económica de los Estados de África Occidental (CEDEAO), la Unión Europea y el Consejo de Europa es limitada, porque esos enfoques se aplican solo a los Estados miembros de las respectivas organizaciones. En la actualidad, el instrumento de mayor alcance es el Convenio sobre la

⁴⁴ Choo, "Organised crime groups", pág. 281; Oficina Europea de Policía (Europol), "Child abuse in relation to trafficking in human beings", Serious Crime Overview, enero de 2008, pág. 2; *Organised Crime Situation Report 2005*, pág. 8; John Carr, *Child Abuse, Child Pornography and the Internet* (Londres, NCH, The Children's Charity, 2004), pág. 17; Canadá, Servicio de Inteligencia Criminal del Canadá, *Annual Report on Organized Crime in Canada 2007* (Ottawa, 2007), pág. 4; "Annual report on organized crime in Greece for the year 2004", *Trends in Organized Crime*, vol. 9, Núm. 2 (2005), pág. 5; Naciones Unidas, Comisión de Derechos Humanos, Informe del Relator Especial sobre la venta de niños, la prostitución infantil y la utilización de niños en la pornografía (E/CN.4/2005/78), pág. 8.

⁴⁵ Choo, "Organised crime groups" pág. 273 (véase la nota de pie de página 40).

⁴⁶ Susan W. Brenner, "Organized cybercrime? How cybercrime may affect the structure of criminal relationships", *North Carolina Journal of Law and Technology*, Núm. 4 (2002), pág. 27.

Ciberdelincuencia, que se considera un instrumento importante en la lucha contra el delito cibernético y cuenta con el apoyo de diferentes organizaciones internacionales. Además, de conformidad con el artículo 37 del Convenio, puede adherirse a él también cualquier Estado que no sea miembro del Consejo. Cuatro Estados no miembros (el Canadá, los Estados Unidos, el Japón y Sudáfrica) participaron en las negociaciones del Convenio, y tres de ellos (el Canadá, los Estados Unidos y el Japón) están estrechamente vinculados al Consejo por su condición de observadores. Al mes de diciembre de 2009 habían firmado el Convenio 46 Estados⁴⁷ (entre ellos los cuatro Estados no miembros que participaron en la negociación); 26 Estados miembros y un Estado no miembro del Consejo la habían ratificado⁴⁸.

33. Los efectos del Convenio sobre la Ciberdelincuencia no pueden medirse únicamente por el número de Estados que lo han firmado o ratificado. La Argentina, Botswana, Egipto, Filipinas, Nigeria y el Pakistán, por ejemplo, han modelado partes de su legislación con arreglo al Convenio, sin adherirse oficialmente a él. Aún así, en comparación con los patrones mundiales, el número y la rapidez de las firmas y las ratificaciones siguen siendo un problema. En los nueve años transcurridos desde que los primeros 30 Estados firmaron el Convenio el 23 de noviembre de 2001, solo otros 16 Estados han pasado a ser signatarios. Desde 2001, ningún Estado no miembro del Consejo de Europa se ha adherido al Convenio, aunque cinco (Chile, Costa Rica, Filipinas, México y la República Dominicana) han sido invitados a hacerlo. El ritmo de la ratificación ha sido igualmente lento: dos Estados (Albania y Croacia) ratificaron el Convenio en 2002, dos (Estonia y Hungría) lo hicieron en 2003, cuatro (Lituania, Eslovenia, la ex República Yugoslava de Macedonia y Rumania) en 2004, tres (Bulgaria, Chipre y Dinamarca) en 2005, siete (Armenia, Bosnia y Herzegovina, los Estados Unidos, Francia, Noruega, los Países Bajos y Ucrania) en 2006, tres (Finlandia, Islandia y Letonia) en 2007, dos (Italia y Eslovaquia) en 2008, y tres (Alemania, República de Moldova y Serbia) en 2009. Puesto que el Convenio, además de ser ratificado, tiene en general que aplicarse, la eficiencia del instrumento depende de la plena adaptación de la legislación nacional de los Estados que lo han ratificado. Además, se requieren pruebas que demuestren la plena adaptación.

⁴⁷ Alemania, Albania, Armenia, Austria, Azerbaiyán, Bélgica, Bosnia y Herzegovina, Bulgaria, Canadá, Chipre, Croacia, Dinamarca, Eslovaquia, Eslovenia, España, Estados Unidos, Estonia, la ex República Yugoslava de Macedonia, Finlandia, Francia, Georgia, Grecia, Hungría, Irlanda, Islandia, Italia, Japón, Letonia, Lituania, Luxemburgo, Malta, Montenegro, Noruega, Países Bajos, Polonia, Portugal, Reino Unido, República Checa, República de Moldova, Rumania, Serbia, Sudáfrica, Suecia, Suiza y Ucrania.

⁴⁸ Alemania, Albania, Armenia, Bosnia y Herzegovina, Bulgaria, Chipre, Croacia, Dinamarca, Eslovaquia, Eslovenia, Estados Unidos, Estonia, la ex República Yugoslava de Macedonia, Finlandia, Francia, Hungría, Islandia, Italia, Letonia, Lituania, Noruega, Países Bajos, República de Moldova, Rumania, Serbia y Ucrania.

2. Debate mundial

34. Otro aspecto de la función de los regímenes regionales como instrumentos para la armonización mundial es la posibilidad de los Estados no miembros de participar. A pesar de la dimensión transnacional del delito cibernético, el impacto en las diferentes regiones del mundo es diferente. Esto reviste particular interés para los países en desarrollo⁴⁹. Los enfoques regionales mencionados en el párrafo 32 *supra* no ofrecen la posibilidad de una participación amplia de Estados no miembros. Si bien el Convenio sobre la Ciberdelincuencia es actualmente el instrumento con el mayor número de Estados miembros, también este Convenio limita la posibilidad de los Estados no miembros de participar. En su artículo 37 se estipula que para poder adherirse a él los Estados deberán consultar con los Estados Contratantes del Convenio y obtener su consentimiento unánime. Además, la participación en el debate sobre posibles enmiendas futuras se limitará a las Partes en el Convenio (artículo 44).

35. La experiencia ha demostrado que los Estados son, por lo general, reacios a ratificar las convenciones o a adherirse a ellas cuando no han contribuido a su elaboración y negociación. Esto ha ocurrido independientemente del tema de que traten las convenciones.

36. En las cuatro reuniones preparatorias regionales del 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal se hicieron llamamientos para que se elaborara una convención internacional sobre el delito cibernético.

37. También se hizo un llamamiento de ese tipo en las reuniones de los jefes de los organismos nacionales encargados de combatir el tráfico ilícito de drogas de África, el Cercano Oriente y el Oriente Medio y Europa, en que se celebraron debates sobre Internet, la recopilación de pruebas electrónicas, la legislación y otros temas. En las reuniones celebradas en otras regiones, los participantes llegaron a la conclusión de que los organismos encargados de hacer cumplir la ley y el poder judicial estaban mal preparados y carecían de la capacidad necesaria para hacer frente a la evolución del delito cibernético y para reunir y utilizar pruebas obtenidas mediante tecnologías cibernéticas en la preparación de los procesos. Hubo acuerdo general en que las leyes nacionales estaban quedando a la zaga y en que se requerían enmiendas para respaldar la investigación, el enjuiciamiento y la condena de los delincuentes sobre la base de pruebas obtenidas mediante la tecnología cibernética. Es urgente que los Estados elaboren normas comunes y cooperen a fin de que las autoridades puedan actuar con eficacia en todas las jurisdicciones para llevar a los delincuentes ante la justicia. El mundo académico también ha hecho llamamientos en favor de la elaboración de un instrumento internacional⁵⁰.

⁴⁹ Véanse, por ejemplo, el informe de la Organización de Cooperación y Desarrollo Económicos, *Spam Issues in Developing Countries* (París, OCDE, 2005), pág. 4. Disponible en <http://www.oecd.org/dataoecd/5/47/34935342.pdf>; y *El ciberdelito: Guía*, pág. 16 (véase la nota de pie de página 2).

⁵⁰ Joachim Vogel, "Towards a global convention against cybercrime", documento presentado en la Primera Conferencia Mundial de Derecho Penal, Guadalajara (México), 19 a 23 de noviembre de 2007; Stein Schjølberg y Solange Ghernaouti-Hélie, *A Global Protocol on Cybersecurity and Cybercrime: An Initiative for Peace and Security in Cyberspace* (Oslo, E-dit, 2009).

3. Respuesta a las tendencias recientes

38. El delito cibernético evoluciona constantemente. Cuando se elaboraron instrumentos regionales tales como la ley modelo del Commonwealth sobre los delitos cibernéticos e informáticos y el Convenio sobre la Ciberdelincuencia, los ataques de redes zombi, el “phishing” y el uso terrorista de Internet en gran escala no se conocían, o no tenían la importancia que tienen hoy. Por consiguiente, esos delitos no se tratan en disposiciones específicas. En las reuniones preparatorias regionales del 12° Congreso se abordó la necesidad de combatir esos nuevos fenómenos, especialmente el uso terrorista de Internet, que abarca desde la propaganda, las comunicaciones y la financiación del terrorismo a través de los servicios de pago por Internet hasta la recopilación de información sobre una víctima potencial. El Equipo especial de lucha contra el terrorismo ha examinado estos fenómenos y las posibles respuestas jurídicas en diversas ocasiones⁵¹.

39. Mientras que, en lo que respecta al derecho penal sustantivo, esos fenómenos pueden tratarse aplicando las disposiciones sobre la interferencia de sistemas o la falsificación informática, la aplicación de los instrumentos procesales contenidos en los instrumentos regionales existentes es mucho más difícil, especialmente porque las tecnologías y los servicios que se ofrecen en Internet (las redes sociales, por ejemplo) han cambiado considerablemente. La interceptación de las comunicaciones que utilizan la tecnología VoIP, la admisibilidad de las pruebas digitales en las causas penales, los procedimientos para investigar los casos en que se ha utilizado tecnología de cifrado o los medios de comunicación anónima son problemas que, pese a ser urgentes, no se están abordando a nivel regional y solo en algunos casos se están tratando a nivel nacional⁵².

40. Es importante que se estudien estos asuntos, porque los instrumentos de investigación tradicionales no suelen servir para investigar los delitos cibernéticos. Un ejemplo de ello es la interceptación de comunicaciones. En los últimos decenios, los Estados han elaborado instrumentos de investigación, tales como las escuchas telefónicas, que les han permitido interceptar comunicaciones telefónicas por telefonía móvil y no móvil. Las llamadas telefónicas tradicionales se suelen interceptar por medio de los proveedores de servicios de telecomunicaciones. Para aplicar el mismo principio a las comunicaciones que utilizan la tecnología VoIP, las autoridades encargadas de hacer cumplir la ley tendrían que interactuar con los proveedores de servicios VoIP. Sin embargo, si esos servicios se basan en la tecnología inter pares⁵³, los proveedores pueden no estar en condiciones de

⁵¹ Véase, por ejemplo, Equipo especial de lucha contra el terrorismo, “Report of the Working Group on Countering the Use of Internet for Terrorist Purposes”, febrero de 2009. Disponible en www.un.org/terrorism/pdfs/wg6-internet_rev1.pdf.

⁵² Véase una reseña de los diferentes enfoques nacionales para tratar estas cuestiones en *El ciberdelito: Guía*, cap. 6 (véase la nota de pie de página 2).

⁵³ La tecnología inter pares permite la conectividad directa entre los participantes en la red, en lugar de obligar a los usuarios a comunicar a través de estructuras centralizadas convencionales basadas en un servidor.

interceptar las comunicaciones, porque los datos en cuestión se transfieren directamente de un interlocutor a otro⁵⁴. Por lo tanto, es posible que se necesiten también nuevas técnicas, además de los instrumentos jurídicos conexos.

41. La capacidad de realizar investigaciones complejas reviste interés no sólo para los nuevos delitos sino también para las formas más tradicionales de delito cibernético, como la pornografía infantil. Desde mediados del decenio de 1990, los distribuidores y consumidores de pornografía infantil tienen acceso a servicios de red que se utilizan de manera cada vez más intensiva⁵⁵. Internet se ha convertido en el principal medio de intercambio de pornografía infantil. Los problemas relacionados con la detección e investigación de los casos de pornografía infantil se conocen desde los años noventa; en gran parte persisten porque los delincuentes pueden hacer uso de una tecnología sofisticada para obstaculizar las investigaciones. Según un estudio, por ejemplo, el 6% de las personas que han sido descubiertas con pornografía infantil utilizaba tecnología de cifrado, el 17% empleaba programas informáticos protegidos por contraseñas, el 3% usaba programas informáticos que eliminan las pruebas y el 2% hacía uso de sistemas de almacenamiento remoto⁵⁶. Además, se ha observado un cambio en lo que respecta a la tecnología: mientras que en los primeros tiempos de Internet predominaba el intercambio a través de canales tradicionales como las multiconferencias, en los últimos tiempos la pornografía infantil ha comenzado a distribuirse con otras tecnologías, como las redes inter pares⁵⁷.

B. Aplicación de la ley

42. Además de necesitar instrumentos jurídicos, la aplicación de la ley depende en gran medida de la disponibilidad de instrumentos de investigación tales como programas informáticos forenses (para reunir pruebas, registrar las pulsaciones de teclado y descifrar o recuperar ficheros suprimidos) y programas informáticos o

⁵⁴ En lo que respecta a la interceptación de comunicaciones con VoIP por los organismos encargados de hacer cumplir la ley, véanse Steven Bellovin y otros, “Security implications of applying the Communications Assistance to Law Enforcement Act to Voice over IP”, 13 de junio de 2006, disponible en www.cs.columbia.edu/~smb/papers/CALEAVOIPPreport.pdf; Matthew Simon y Jill Slay, “Voice over IP: forensic computing implications”, documento presentado en la cuarta Conferencia australiana sobre técnicas forenses digitales, Perth (Australia), diciembre de 2006.

⁵⁵ Estados Unidos, Cámara de Representantes, “Sexual exploitation of children over the Internet” (2007), 109º Congreso, pág. 9.

⁵⁶ Janis Wolak, David Finkelhor y Kimberly J. Mitchell, *Child Pornography Possessors Arrested in Internet-Related Crime: Findings From the National Juvenile Online Victimization Study* (Alexandria, Virginia, National Center for Missing and Exploited Children, 2005), pág. 9.

⁵⁷ Estados Unidos, Oficina General de Contabilidad, *File-Sharing Programs, Child Pornography is Readily Accessible over Peer-to-Peer Networks*, testimonio prestado ante el Comité de Reforma del Gobierno, Cámara de Representantes, Informe de la Oficina General de Contabilidad GAO-03-537T (Washington, D.C., marzo de 2003); Gretchen Ruethling, “27 charged in international online child pornography ring”, *New York Times*, 16 de marzo de 2006; Choo, “Organised crime groups”, pág. 282 (véase la nota de pie de página 40); Reino Unido, Stockport Safeguarding Children Board, *Safeguarding Children in Stockport: Policy and Practice Handbook* (mayo de 2008), pág. 299, disponible en <http://www.safeguardingchildreninstockport.org.uk/documents/Section%2000%20-%20Preface%20and%20contents.pdf>.

bases de datos de gestión de la investigación (por ejemplo, con valores “hash” para imágenes de pornografía infantil conocidas). En los últimos años se han desarrollado varios instrumentos de ese tipo y se sigue trabajando en ello⁵⁸. Por ejemplo, en el Colegio Universitario de Dublín se está realizando un proyecto de investigación titulado “Automatic Event Reconstruction for Digital Forensics and Intrusion Analysis” (véase la información disponible en <http://cci.ucd.ie/?q=node/33>), y en diciembre de 2009 se introdujo en los Estados Unidos una nueva tecnología para localizar la pornografía infantil denominada PhotoDNA. Uno de las cuestiones más importantes relacionadas con el desarrollo de esos instrumentos sigue siendo la necesidad de que los encargados del desarrollo coordinen los trabajos para evitar la duplicación. Del mismo modo, deben coordinarse también los esfuerzos de las redes de puntos de contacto (como las del Grupo de los Ocho y de la INTERPOL, y la red vinculada al Convenio sobre la Ciberdelincuencia).

C. Fomento de la capacidad

43. El delito cibernético es un problema no sólo en los países desarrollados sino también en los países en desarrollo. Según la Development Gateway Foundation, en 2005 había más usuarios de Internet en los países en desarrollo que en las naciones industrializadas⁵⁹. El hecho de que la CEDEAO haya adoptado recientemente una directiva sobre el delito cibernético y de que la Comunidad del África Oriental haya presentado un proyecto de marco para la ciberlegislación es una señal positiva. Un mayor apoyo podría ayudar a los organismos encargados de hacer cumplir la ley a prepararse para los delitos que puedan cometerse cuando un mayor número de usuarios disponga de acceso de banda ancha en el mundo en desarrollo. La Asamblea General, en su resolución 64/179, titulada “Fortalecimiento del Programa de las Naciones Unidas en materia de prevención del delito y justicia penal, en particular de su capacidad de cooperación técnica”, señaló las nuevas cuestiones de política citadas en el informe del Secretario General (A/64/123), a saber, la piratería, el delito cibernético, la explotación sexual de niños y la delincuencia urbana, e invitó a la UNODC a que, de conformidad con su mandato, estudiara el modo de hacer frente a esas cuestiones.

D. Capacitación

44. Puesto que investigar los delitos cibernéticos y enjuiciar a las personas involucradas en ellos plantea dificultades especiales, es importante impartir capacitación a los funcionarios encargados de hacer cumplir la ley, los fiscales y los jueces. Como se recalcó en la reunión de un grupo de expertos de la UNODC sobre el delito cibernético, celebrada en Viena los días 6 y 7 de octubre de 2009, la mayoría de las organizaciones internacionales y regionales que se ocupan del asunto

⁵⁸ Véase, por ejemplo, el proyecto de investigación titulado “Automatic Event Reconstruction for Digital Forensics and Intrusion Analysis” que se está llevando a cabo en el Colegio Universitario de Dublín (información disponible en <http://cci.ucd.ie/?q=node/33>).

⁵⁹ Información disponible en <http://topics.developmentgateway.org/special/informationociety>.

han adoptado medidas para capacitar a los expertos que participan en la investigación de los delitos cibernéticos y para elaborar material didáctico⁶⁰.

IV. Conclusiones y recomendaciones

45. Investigar los delitos cibernéticos y enjuiciar a sus autores es difícil para todas las instituciones que intervienen en ello. Habida cuenta de la complejidad de la cuestión y del constante desarrollo técnico, la capacitación sostenida y cada vez más amplia de todas las autoridades interesadas sigue siendo un aspecto crucial. El debate sostenido en la reunión de 2009 del grupo de expertos de la UNODC sobre el delito cibernético indicó que el fomento de la capacidad institucionalizado y la sostenibilidad a largo plazo eran dos factores clave para medir el éxito de las iniciativas futuras.

46. A fin de eliminar los refugios seguros y mejorar la cooperación internacional, debería prestarse atención a colmar las lagunas en la legislación vigente y promover la cohesión, la coherencia y la compatibilidad de las leyes. Habida cuenta de la importancia de armonizar la legislación y sacar provecho de los resultados de las reuniones preparatorias del 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, debería darse una consideración atenta y favorable a la elaboración de una convención mundial contra el delito cibernético.

47. Entretanto, la UNODC, en su calidad de órgano encargado de establecer normas en relación con la prevención del delito y la justicia penal, ofrecerá una plataforma multilateral en que se prestará atención preferente a los países en desarrollo. La Oficina seguirá adoptando un enfoque amplio, multidisciplinario y basado en la colaboración, aunando sus comprobados conocimientos en los sectores jurídico, técnico y de aplicación de la ley para combatir las actividades delictivas con la competencia técnica específica y bien desarrollada de los asociados clave que ya trabajan en la lucha contra el delito cibernético. La UNODC trabajará con los expertos y los instrumentos adecuados, incluidos los del sector privado (en particular los proveedores de servicios de Internet) para combatir el problema en un determinado país o región. Se concederá prioridad a la prestación de asistencia técnica a los Estados miembros que la necesiten, con vistas a subsanar la falta de capacidad y competencia técnica y a asegurar la sostenibilidad a largo plazo de la lucha contra los delitos informáticos.

⁶⁰ Por ejemplo, la iniciativa de cooperación económica en Asia y el Pacífico ha organizado varias actividades de capacitación sobre el delito cibernético, incluida la legislación sobre esos delitos; el Commonwealth ha organizado sesiones de formación jurídica y técnica; el Consejo de Europa ha contribuido a actividades de formación en diversas partes del mundo y ha elaborado material didáctico específico para los jueces; la Unión Europea ha respaldado el desarrollo de materiales y sesiones de formación sobre el delito cibernético para los organismos encargados de hacer cumplir la ley de sus Estados miembros y ha organizado varias sesiones de capacitación dentro y fuera de Europa; la INTERPOL ha organizado varias sesiones de capacitación para los organismos encargados de hacer cumplir la ley y ha elaborado material didáctico; la UIT ha preparado material didáctico sobre el delito cibernético que está disponible en todos los idiomas de las Naciones Unidas, ha impartido capacitación general en varias actividades regionales y ha ofrecido formación específica para los jueces.

48. Concretamente, la UNODC procurará: ayudar a los Estados miembros a adoptar legislación para investigar eficazmente los delitos informáticos y enjuiciar a sus autores; aumentar los conocimientos operacionales y técnicos de los jueces, los fiscales y los funcionarios encargados de hacer cumplir la ley sobre las cuestiones relacionadas con el delito cibernético, mediante la capacitación, la adaptación o el desarrollo de material didáctico relativo a la investigación de los delitos informáticos y el enjuiciamiento de sus autores, etc.; formar a las autoridades encargadas de hacer cumplir la ley para que utilicen eficazmente los mecanismos de cooperación internacional en la lucha contra el delito cibernético; sensibilizar a la sociedad civil e impulsar a las autoridades decisorias a unir sus esfuerzos para prevenir y combatir los delitos cibernéticos; y determinar y difundir las buenas prácticas y promover la colaboración entre los sectores público y privado para prevenir y combatir esos delitos.
