Naciones
Unidas

A/CONF.203/14

11º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal

Bangkok, 18 a 25 de abril de 2005

Distr.: General
14 de marzo de 2005

Español
Original: inglés

Tema 3 del programa provisional*
Medidas eficaces contra la delincuencia organizada transnacional

Medidas para combatir los delitos informáticos**

Documento de antecedentes***

Resumen

La proliferación de nuevas tecnologías de la información y las comunicaciones en todo el mundo ha dado lugar a más formas de delitos informáticos, que amenazan no sólo a la confidencialidad, la integridad, o la disponibilidad de los sistemas de computadoras, sino también a la seguridad de la infraestructura esencial. La innovación tecnológica también da lugar a pautas diferentes de innovación delictiva; en consecuencia, diferentes amenazas de delitos informáticos reflejan diferencias en todo el espectro de la denominada "brecha digital". Cuando se combaten esos delitos, varios problemas forenses —que surgen en parte de pruebas digitales intangibles y transitorias— plantean desafíos a los investigadores, los fiscales y los jueces por igual. Es más, la investigación y la interposición de una acción judicial eficaz respecto de delitos informáticos a menudo requieren el seguimiento de la actividad delictiva y sus efectos a través de una diversidad de compañías o proveedores de servicio de Internet, a veces a través de fronteras nacionales, que pueden dar lugar a cuestiones difíciles de jurisdicción y soberanía.

La complejidad de los retos específicos que plantean los delitos informáticos requiere la cooperación internacional que depende, en último término, de que los países estén dotados de los necesarios instrumentos jurídicos, procesales y reglamentarios. En los últimos años se han iniciado actividades regionales e interregionales para desarrollar métodos eficaces de cooperación internacional para combatir delitos informáticos que han dado lugar a varios logros significativos. Para llevar esos esfuerzos a buen término, es necesario apoyar una gama amplia de actividades de investigación sobre los diversos aspectos de la lucha contra los delitos

* A/CONF.203/1.

** El Secretario General desea expresar su reconocimiento al Instituto Coreano de Criminología y al Gobierno del Canadá por la asistencia prestada en la organización del Seminario 6.

*** La necesidad de realizar más investigaciones y consultas demoró la presentación del documento.

V.05-82262 (S) 140405 150405

informáticos para fomentar una asociación activa entre el gobierno y el sector privado.

En el presente documento de antecedentes se destacan los retos planteados por los delitos informáticos para que los participantes en el Seminario 6 puedan considerar las recomendaciones hechas por las reuniones preparatorias regionales del 11º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal y desarrollar un plan para una respuesta mundial efectiva.

Índice

I. Introducción

1. Las tecnologías de la información y las comunicaciones están transformando las sociedades en todo el mundo. La innovación está creando mercados nuevos para los bienes y los servicios. Estas tecnologías están revolucionando los procesos laborales, mejorando la productividad en las industrias tradicionales y reconfigurando la velocidad y el flujo de los capitales. No obstante, los cambios económicos son sólo un factor de la ecuación. Las sociedades también están experimentando cambios culturales profundos: dan forma y a su vez son conformadas por los medios de difusión y se adaptan al crecimiento explosivo de la Internet. La multiplicación mundial de nuevas tecnologías de la información y las comunicaciones también proyecta una oscura sombra: ha posibilitado nuevas formas de explotación, nuevas oportunidades para las actividades delictivas y por cierto nuevas formas de delincuencia.

2. Las cuatro reuniones preparatorias regionales para el 11º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal propusieron varias recomendaciones para su examen en el 11º Congreso, entre ellas: a) examinar la experiencia actual y los marcos jurídicos y acuerdos nacionales existentes para la cooperación entre los Estados, así como entre los Estados y los proveedores de servicios de Internet; b) examinar las maneras más apropiadas de promover la cooperación y el intercambio de experiencias y conocimientos técnicos especializados entre los gobiernos y el sector privado para el establecimiento y la utilización de mecanismos para prevenir y combatir los delitos informáticos y garantizar la seguridad de las redes de computadoras y los sistemas de comunicación y la existencia de mecanismos de respuesta apropiados; c) explorar los medios de mejorar la capacidad de los gobiernos de desarrollar y aplicar técnicas de investigación especiales y capacidades de enjuiciamiento adecuadas, incluso elaborando y aplicando programas de capacitación integrales para oficiales de justicia penal; d) combatir la utilización de la tecnología de las computadoras para explotar a las mujeres y los niños, especialmente en relación con la pornografía y la pedofilia; e) examinar la viabilidad de establecer un equipo de tareas mundial de la Internet para la cooperación internacional en la lucha contra los delitos informáticos; y f) considerar la posibilidad de proponer la negociación de una nueva convención contra los delitos cibernéticos con miras a sentar las bases para una acción colectiva eficaz contra esta forma de actividad delictiva[1].

El concepto de “delitos informáticos” o términos similares como “delitos cibernéticos” ha sido un tema de debate durante los últimos 30 años. El prototipo se remonta a un informe del Instituto de Investigación de Stanford[1] y reapareció en forma ligeramente modificada en 1979[2] y en 1989[3]. El esquema de organización se utilizó ampliamente en artículos posteriores sobre la delitos cibernéticos: la computadora como sujeto de un delito, o la computadora como un instrumento (la cuarta función, propuesta en 1973, la computadora como símbolo, parece haber desaparecido en los años 80). Una reformulación útil de este modelo conceptual es considerar los delitos informáticos como una conducta proscrita por la legislación y/o la jurisprudencia que a) ataca a las propias tecnologías de la computación y

las comunicaciones; b) incluye la utilización de tecnologías digitales en la comisión del delito; o c) incluye la utilización incidental de las computadoras en la comisión de otros delitos y, en consecuencia, la computadora pasa a ser una fuente de datos digitales probatorios[4]. Las leyes y los tratados, incluido el Convenio sobre el Delito Cibernético del Consejo de Europa[5], han definido diversos tipos de delitos informáticos (como un delito contra la confidencialidad, la integridad o la disponibilidad de los sistemas de computadoras; delitos relacionados con el contenido; y delitos relacionados con la propiedad intelectual).

II. Delitos informáticos

3. Hay algunas formas de delitos informáticos que atacan a las propias tecnologías de la información y las comunicaciones, y a los que algunas veces se hace referencia como delitos contra la confidencialidad, la integridad o la disponibilidad de sistemas de computadoras. Éstos incluyen formas de robo de servicios de telecomunicación y robo de servicios de computación utilizando diversas técnicas de piratería (según la tecnología, estos incluyen acceso no autorizado, robo de códigos y contraseñas, clonación digital, robo de la información contenida en la banda magnética de la tarjeta de crédito (*skimming*) y otros). Los servidores y los sitios web pueden ser blancos de ataques de servicios. En algunos casos, esos delitos son el resultado de los ataques distribuidos de denegación de servicio en que docenas o cientos de computadoras comprometidas se utilizan como "zombies" para bombardear el blanco escogido con peticiones tan numerosas que no se puede atender a ninguna. En otros casos, la denegación de servicio surge de las avalanchas de encomiendas ("*packet storms"*) creadas mediante la reproducción descontrolada de parásitos (programas informáticos que se duplican automáticamente), que en pocos minutes crean miles de millones de copias de ellos mismos; el mero volumen tapona hasta los circuitos de fibra óptica más anchos y produce el colapso de los masivos sistemas de computadoras institucionales. Durante los dos últimos decenios, las epidemias mundiales de virus informáticos han interrumpido las redes comerciales y de consumidores; periódicamente aparecen nuevos tipos de parásitos y virus particularmente virulentos y perjudiciales. Los ejemplos recientes revelan los dos extremos de la especialización: en un extremo están los parásitos adaptados a una población destinataria de decenas de millones de sistemas de computadoras que funcionan con los sistemas operativos y las aplicaciones más populares; en el otro, hay parásitos diseñados para atacar únicamente las aplicaciones de seguridad sumamente complejas que se utilizan en sólo unos pocos miles de plataformas.

Dos residentes de Melbourne (Australia) enviaron entre 6 y 7 millones de mensajes de correo electrónico a direcciones de Australia y los Estados Unidos de América y colocaron numerosos mensajes en los tableros de mensajes de los principales proveedores de servicios de Internet. La finalidad de esas comunicaciones era promover la compra de acciones de una empresa de los Estados Unidos que se comerciaban en los Estados Unidos en la bolsa de valores NASDAQ (National Association of Securities Dealers Automated Quotations Exchange) Los mensajes, que se enviaron con remitentes falsos y se retransmitieron a través de servidores de terceros, anunciaban un aumento de precios de hasta un 900 por ciento en las acciones de la empresa. Poco tiempo después, el volumen de venta de las acciones aumentó 10 veces y su precio se duplicó antes de que se suspendieran las ventas y la empresa negara las declaraciones hechas en las diversas comunicaciones.

Los dos residentes habían realizado un clásico fraude de "inflar y vender": uno de los cómplices, que era accionista en la empresa, sabía que estaba comunicando información falsa; cuando aumentó el precio de la acción de la empresa, vendió sus acciones con beneficio.

Los dos individuos habían infringido las leyes tanto de Australia como de los Estados Unidos. Además de la manipulación de la bolsa de valores, el volumen de tráfico generado por el correo electrónico *spam* fue suficiente constituir una interferencia en la utilización legal de una computadora. La Comisión de Valores e Inversiones (ASIC) de Australia actuó en respuesta a las demandas del público australiano, y a la información proporcionada por las autoridades de los Estados Unidos. Se siguió la pista de los mensajes de correo electrónico distribuidos por los autores a través de redes comerciales desprevenidas y la pista financiera del pago por los servicios de Internet.

Como era usual para los delitos de esta naturaleza, la Comisión de Títulos y Valores de los Estados Unidos procuró la restitución de las ganancias ilícitas y un mandato judicial temporal y permanente para impedir que los dos cómplices repitieran sus actividades. Se les exigió que devolvieran sus ganancias conseguidas ilícitamente y que prometieran que nunca más incurrirían en tal conducta. Las autoridades de los Estados Unidos confiaban en la capacidad de Australia para manejar las actuaciones penales en Australia. La ASIC presentó 19 cargos penales contra los dos acusados. Ambos se declararon culpables de difundir información falsa o materialmente engañosa, que probablemente induciría la compra de los títulos, y la interferencia, interrupción u obstrucción de la utilización lícita de una computadora. Ambos recibieron penas de prisión de dos años, que se suspendieron (en el caso del principal infractor, después de haber pasado tres meses en custodia).

4. En el contexto institucional, la privación del acceso a los datos comprende desde las circunstancias donde los datos quizá sean recuperables (por ejemplo, un ataque de un empleado disgustado que realiza un cifrado no autorizado de ficheros de datos), a la destrucción no recuperable de los datos (o sea, no la supresión

sencilla de ficheros sino la supresión física y/o destrucción de los discos duros u otros medios de almacenamiento que contienen los ficheros). Las redes de área locales (LAN) inalámbricas, que fueron adoptadas rápidamente por las empresas en los últimos años, pueden ser vulnerables a los ataques de denegación de servicio (como la interferencia (*jamming*)) aun cuando estén protegidas contra un acceso no autorizado[6].

5. También es importante que se tenga conciencia de la forma en que las computadoras se utilizan como instrumentos o medios para cometer delitos. La delincuencia relacionada con la modificación de datos tiene muchas variantes, entre ellas los actos maliciosos que resultan delictivos, como el vandalismo electrónico ("*defacement*") de un sitio web y otros que constituyen falsificación profesional. Hay sitios web dedicados al "*carding*" (falsificación de tarjetas de crédito), que incluye la producción de moneda falsificada de gran calidad y pasaportes. El robo de datos[7] abarca un espectro amplio, desde la piratería de información y el espionaje industrial hasta la trasgresión de derechos de autor (robo de propiedad intelectual en forma de programas informáticos pirata, ficheros de música[8], vídeo digital y otros). El robo de datos quizá no sea sencillamente un delito económico; también puede violar la privacidad y los derechos conexos del individuo en los nuevos delitos asociados con el robo de la identidad.

6. Hay muchos tipos de delitos relacionados con las computadoras, incluidos el robo económico, como los ataques de piratería contra bancos o sistemas financieros, o el fraude, incluida la transferencia electrónica de fondos. También se han expresado inquietudes con respecto al blanqueo electrónico de capitales y cuestiones afines, como la evasión tributaria.

7. Las computadoras también se utilizan para facilitar una gama amplia de ventas telefónicas y fraude de inversiones con prácticas engañosas. Según un informe amplio preparado en los Estados Unidos para el año 2003[9], el fraude de subasta es el fraude relacionado con las computadoras que se denuncia con más frecuencia en las reclamaciones de los consumidores, y representa el 61% de las reclamaciones por fraude. Otras formas de fraude a los consumidores pertenecen a la categoría más genérica de "falta de entrega del producto o falta de pago" que sigue a una transacción en la Internet. El fraude de títulos, asociado con la manipulación en la bolsa de valores de inversiones de valor bajo, es todavía relativamente raro a nivel de los consumidores.

> En febrero de 2000, un joven canadiense de 15 años de edad obtuvo el control de varias computadoras y las utilizó para distribuir un ataque de denegación de servicio contra Yahoo, Amazon.com y otros conocidos sitios de comercio electrónico. Al limitar o hacer más lento el acceso a esos sitios web, causó perjuicios a los propietarios por valor de varios millones de dólares por concepto de ventas perdidas, capitalización del mercado y costo de instalar sistemas de seguridad avanzados. Después de hacer alarde de los ataques en varios espacios de tertulias, el joven fue identificado por la Oficina Federal de Investigaciones de los Estados Unidos, que remitió el caso a la Real Policía Montada Canadiense. Muy pocos países, si alguno,

están dispuestos a extraditar a jóvenes y, en este caso, las leyes canadienses prohibían la extradición de un joven. En septiembre de 2001, fue sentenciado a ocho meses de reclusión en un centro de detención juvenil.

8. La "pesca" de información o "*phishing*" (o inundación de mensajes supuestamente de origen conocido (*spoofing spam*)) es la creación de mensajes de correo electrónico con páginas web diseñadas en forma similar a sitios de consumidores existentes. Igual que la basura informática (*spam*), se distribuyen millones de esos mensajes de correo electrónico fraudulentos; ahora bien, en lugar de solicitar directamente la compra de productos o servicios, los mensajes simulan provenir de bancos, subastas en línea y otros sitios legítimos y procuran inducir engañosamente a los usuarios a que respondan comunicando datos personales o financieros o contraseñas. Esa información personal se utiliza luego para realizar compras fraudulentas (a veces después de que la información se ha vendido a un tercero).

9. Delitos ya tipificados, como la extorsión (amenaza de divulgar información comercial o personal o dañar datos o sistemas) y el acoso, también se realizan en línea. También ha habido casos de difamación o calumnia que se descubrieron y sometieron con éxito a la justicia.

10. Hay una variedad de delitos relacionados con el contenido en que se usan computadoras, en particular la difusión de material ilícito y nocivo. Preocupa en particular a la comunidad internacional el problema de la pornografía infantil. Aunque este tipo de pornografía ha existido durante muchas décadas (en forma de fotografías, revistas, películas y vídeos), desde fines del decenio de 1980 ha habido una tendencia creciente a distribuir pornografía infantil mediante una diversidad de redes de computadoras, utilizando diversos servicios de Internet, incluidos los sitios web, los grupos de noticias Usenet, los sistemas de conversación IRC, y las redes entre pares (P2P)[10]. Estas redes se han utilizado para facilitar intercambios de información, comerciar en imágenes o vídeos de pornografía infantil, realizar transacciones monetarias y trasmitir información con respecto al turismo sexual infantil. Una cierta proporción de la distribución de pornografía infantil tiene fines comerciales (más que de intercambio no monetario entre pedófilos) y está vinculada a la delincuencia organizada transnacional. Hay también una zona gris no tan claramente definida, en que la ilegalidad trasciende a una esfera por lo general permisible, dado que la Internet se ha usado durante los últimos 25 años para distribuir pornografía, gran parte de ella de carácter legítimo en muchas jurisdicciones y gran parte de tipo comercial, a la que con frecuencia se denomina "industria del entretenimiento para adultos"[11]. Con todo, hay otros casos que están más claramente definidos; ciertas representaciones que constituyen pornografía (ya sea en forma de imágenes digitales o vídeos) se consideran legalmente obscenas en muchos países y la distribución de material obsceno de ese tipo se considera un delito. La Internet se ha utilizado también para otros delitos de contenido, como la distribución de propaganda de material motivado por los prejuicios y la xenofobia[12].

Entre los casos más conocidos del decenio de 1990 figura un ataque contra el Citibank, realizado por un joven de la Federación de Rusia que obtuvo acceso no autorizado a servidores del banco en los Estados Unidos. El perpetrador obtuvo la colaboración de cómplices para abrir cuentas bancarias en todo el mundo, y luego dio instrucciones a la computadora del Citibank para que transfiriera fondos a las diversas cuentas. Cuando se descubrió el plan y se identificó al presunto perpetrador, un tribunal federal de los Estados Unidos emitió un mandamiento de detención. En ese momento, no había un tratado de extradición entre la Federación de Rusia y los Estados Unidos, pero el acusado cometió el error de visitar el Reino Unido para asistir a una feria de informática. En virtud de los arreglos de extradición en vigor entre el Reino Unido y los Estados Unidos, las autoridades británicas podían prestar asistencia en la medida en que el delito del que se acusaba al joven tuviera un equivalente en el derecho británico. El acusado presentó un recurso de hábeas corpus, impugnando la extradición con el argumento, entre otros, de que la apropiación ilícita había tenido lugar en la Federación de Rusia, donde estaba ubicado el teclado de su computadora, y no en los Estados Unidos. El tribunal sostuvo que la presencia física del acusado en San Petersburgo era menos importante que el hecho de que había utilizado discos magnéticos ubicados en los Estados Unidos. Además, los actos de los que había sido acusado tenían claros equivalentes en la Ley de abuso de la informática del Reino Unido, de 1990; si hubiera operado desde el Reino Unido en lugar de la Federación de Rusia, los tribunales británicos habrían tenido jurisdicción. El acusado fue extraditado a los Estados Unidos, donde fue declarado culpable y condenado a pena de prisión.

11. En los últimos años se ha prestado cada vez más atención a la relación entre el terrorismo y la Internet, aunque también en este caso hay una gran diversidad de actividades. Hay indicios de que la Internet se utiliza para facilitar la financiación del terrorismo y como instrumento logístico para planificar y ejecutar actos de terrorismo. También se presta más atención a la función de la Internet en la difusión de propaganda terrorista y en el uso de la Internet para el reclutamiento. Esas actividades son distintas del terrorismo cibernético, que ha sido definido por el Centro Nacional de Protección de la Infraestructura de los Estados Unidos como un "acto delictivo perpetrado con el uso de computadoras que resulta en violencia, muerte y/o destrucción, y que crea terror con el propósito de ejercer presión sobre un gobierno para que cambie sus políticas"[13]. Hay dos esferas concretas de preocupación: los ataques contra datos de importancia fundamental y los ataques contra infraestructura crítica.

12. Se tiene cada vez más conciencia de la importancia que reviste la infraestructura de información crítica, redes que no sólo hacen posible las comunicaciones sino que también se utilizan para administrar y controlar aspectos fundamentales de otras infraestructuras críticas, como la energía, el transporte, los alimentos y la salud pública. En muchos países de todo el mundo, la infraestructura crítica puede estar en manos privadas y ser especialmente vulnerable porque

muchos de sus sistemas de control dispersos y sus sistemas de adquisición de datos y supervisión están conectados a la Internet, desde donde pueden ser atacados. Dada la creciente interdependencia de las sociedades modernas, los ataques cibernéticos contra ese tipo de infraestructura pueden tener graves repercusiones inmediatas en todo el sistema económico y político nacional, así como profundos efectos transnacionales. Es esencial estar en condiciones de repeler esos ataques contra la infraestructura de información crítica (ya sean motivados por actividades terroristas o por otras actividades delictivas), a fin de reducir al mínimo el grave riesgo de que se produzcan efectos en cascada sobre otras infraestructuras esenciales para la sociedad.

13. Los retos que plantean los sistemas avanzados de cifrado de datos, que están ampliamente disponibles y que fueron objeto de la atención internacional en los últimos cinco años, todavía no se han resuelto y la nueva generación de criptografía cuántica ya se vislumbra en el horizonte[14]. Aunque la criptografía es esencial para los negocios y el comercio electrónico, también ha sido utilizada por los delincuentes. El dilema de la "tecnología de uso doble" va más allá de la esteganografía y afecta a variedades de programas informáticos de redes entre pares, que son gratuitos y están reforzados con un fuerte cifrado muy resistente a la censura (por ejemplo, Freenet). Esa tecnología, promueve la libertad de expresión y puede contribuir a promover las libertades democráticas, pero también puede ser utilizada por delincuentes para ocultar sus comunicaciones o distribuir material ilícito.

III. La brecha digital y los delitos relacionados con las computadoras

14. Cuando las tecnologías de la información y las comunicaciones se difunden a diferentes partes del mundo, esa dispersión no es uniforme. Mientras en una zona se puede observar el tendido de cables de fibra óptica de alta capacidad, en otras pueden estar aumentando rápidamente las redes móviles e inalámbricas. Las diferentes pautas de adaptación tecnológica exponen a las regiones a diferentes tipos de vulnerabilidades, y aparecen clases específicas de delitos relacionados con las computadoras para aprovechar las circunstancias diferentes.

15. El cambio ha sido trascendental: un aumento monumental de la cantidad de dispositivos de tecnologías de la información y las comunicaciones (hay actualmente unos 2.000 millones de computadoras y otras piezas de equipo con microprocesadores en todo el mundo); el crecimiento exponencial de la conectividad; avances revolucionarios en la ciencia de la computación, como los avances decisivos en miniaturización, velocidad y capacidad de almacenamiento; la aparición de sistemas inteligentes y la robótica; y una mayor interacción entre los seres humanos y las computadoras. Con todo, esta transformación tecnológica no sólo se difunde, vinculando a las personas, los objetos y la información de una manera sin precedentes, sino que también trae consigo la siguiente generación de amenazas y vulnerabilidades digitales y requiere una revisión dramática de la forma en que se considera la delincuencia en el siglo XXI.

16. Ante esta situación, la Asamblea General promovió en 2002 nuevas actividades internacionales para ayudar a los Estados Miembros a combatir la

delincuencia relacionada con las computadoras. En los planes de acción para la aplicación de la Declaración de Viena sobre la delincuencia y la justicia: frente a los retos del siglo XXI, anexa a la resolución 56/261 de la Asamblea General, de 31 de enero de 2002, una sección especial se titula "Medidas contra los delitos relacionados con la alta tecnología y la informática"; en esa sección se hacen recomendaciones sobre políticas orientadas hacia la acción, para prevenir y combatir esos tipos de delincuencia. En su resolución 57/170, de 18 de diciembre de 2002, la Asamblea invitó a la Comisión de Prevención del Delito y Justicia Penal a que, al formular recomendaciones con respecto al 11° Congreso con arreglo a lo dispuesto en la resolución 56/119 de la Asamblea General, de 19 de diciembre de 2001, tuviera en cuenta los progresos realizados en el seguimiento de la Declaración de Viena y los planes de acción.

17. El reconocimiento de la brecha digital ha sido uno de los pilares de las aportaciones de las Naciones Unidas al inicio del siglo XXI. El contexto general está dado por la Declaración del Milenio de las Naciones Unidas, aprobada por la Asamblea General en su resolución 55/2, de 8 de septiembre de 2000. En virtud del objetivo 8 de los objetivos de desarrollo del Milenio, anexo al informe del Secretario General titulado "Guía general para la aplicación de la Declaración del Milenio" (A/56/326), figura la meta 8, "En colaboración con el sector privado, velar por que se puedan aprovechar los beneficios de las nuevas tecnologías, en particular de las tecnologías de la información y de las comunicaciones". En la Declaración de Principios aprobada en la Cumbre Mundial sobre la Sociedad de la Información, celebrada en Ginebra del 10 al 12 de diciembre de 2003, hay una visión común de la sociedad de la información (A/C.2/59/3, cap. I, secc. A): "Somos plenamente conscientes de que las ventajas de la revolución de la tecnología de la información están en la actualidad desigualmente distribuidas entre los países desarrollados y en desarrollo, así como dentro de las sociedades. Estamos plenamente comprometidos a convertir la brecha digital en una oportunidad digital para todos, especialmente aquellos que corren peligro de quedar rezagados y aún más marginados"[15].

> Al final de 2004, el acceso a la Internet en China había llegado a 94 millones de personas, o aproximadamente el 7,2% de la población de ese país, de los cuales el 45,5% tenía acceso de banda ancha. Se estimaba que había 41,6 millones de sistemas anfitriones, 60 millones de direcciones IPv4 (versión 4 del protocolo de Internet), 432.077 nombres de dominio y 668.900 sitios web cn (sitios web chinos)[16]. Con una tasa de crecimiento anual de un 18%, el número de usuarios de Internet en China superará al de América del Norte en 2008 y ya supera al número de usuarios de Internet del Japón y la República de Corea combinados. En 1999, había sólo 8,9 millones de usuarios; ese número aumentó a 33,7 millones en 2001. El número de sistemas anfitriones aumentó de 3,5 millones en 1999 a 33,7 millones en 2001.

18. Al final de 1985, el número de sistemas anfitriones de Internet superaba los 2000; en 1989 había alcanzado la cifra de 100.000 y en 1990 había superado los 300.000. El millón se alcanzó a mediados de 1992, los 10 millones a fines de 1995 o

principios de 1996 y los 100 millones a finales de 2000; en julio del 2002, esa cifra había llegado a 162 millones[17]. En 2002, el mundo en desarrollo tenía sólo 4,1 usuarios de Internet y 3,3 computadoras personales por cada 100 habitantes, mientras que en el mundo desarrollado esas cifras eran 33,3 y 36,2 respectivamente (E/2004/62 y Corr.1). Una quinta parte de las personas que vivían en países de altos ingresos tenía el 81,9% de las computadoras personales del mundo, representaba el 76,2% de los usuarios de Internet del mundo y tenía el 97,5% de los sistemas anfitriones de Internet del mundo[18].

19. La mayoría de los países en desarrollo no tienen un sector de telecomunicaciones capaz de apoyar esos sistemas dinámicos, modernos y eficientes de información y comunicaciones. En 2000, las Naciones Unidas comunicaron que sólo un 4,5% de la población mundial tenía acceso a redes, en comparación con el 44% de los norteamericanos y el 10% de los europeos, mientras que las tasas en África, Asia y América del Sur variaban de 0,3% a 1,6%[19]. Actualmente, más del 98% del ancho de banda del protocolo mundial de Internet a nivel regional conecta desde y hacia América del Norte. Cincuenta y cinco países representan el 99% de los gastos mundiales en producción de tecnología de la información (E/200/52, párrs. 50 y 51). Hay una clara tendencia hacia economías basadas en los conocimientos, pero algunos factores distintos del desarrollo, como el costo de la estructura y el acceso a servicios de telecomunicaciones, influyen sobre las tasas de acceso y de uso.

20. Con todo, los beneficios de las tecnologías de la información y las comunicaciones comienzan a difundirse más ampliamente, y esto requerirá un aumento de la toma de conciencia de las amenazas y vulnerabilidades concomitantes relacionadas con los delitos cibernéticos. La brecha digital no sólo marca diferencias económicas entre países desarrollados, países en desarrollo y países con economías en transición[20], sino que revela también pautas diversas en las amenazas y las vulnerabilidades planteadas por los delitos cibernéticos. Las tecnologías de la información y las comunicaciones son adoptadas en diferentes momentos en diferentes regiones, no sólo debido a divergencias entre los ricos y los pobres, sino también en razón de factores como la geografía regional. Por ejemplo, en algunos países con terreno montañoso, el costo de tender cables subterráneos de telecomunicaciones puede ser prohibitivo, y el establecimiento de sistemas de antenas y torres de retransmisión de microondas da lugar a la adopción eficiente de redes de telefonía inalámbrica. En este sentido, las pautas de las tecnologías de la información y las comunicaciones en un país o región pueden ser bastante diferentes de las de una región o país vecino. Las diferencias en la adopción de las innovaciones tecnológicas da lugar a pautas diferentes de innovaciones delictivas y, por lo tanto, a diferentes amenazas de la delincuencia relacionada con las computadoras.

21. Con una infraestructura de telecomunicaciones mínima, un país en desarrollo, puede ser utilizado como trampolín para ataques o como país de tránsito para la preparación de los ataques, en particular si no hay sanciones penales que desalienten los delitos cibernéticos o esas acciones no son enjuiciables. En el caso de los países en desarrollo, los tipos de tecnologías que se despliegan y mantienen inicialmente pueden dar lugar a nuevas amenazas para la región de que se trate. Hay quienes opinan que las estructuras emergentes y todavía frágiles de tecnología de la

información pueden ser desproporcionadamente vulnerables hasta que los sistemas adquieran robustez y las normas de seguridad estén más arraigadas[21].

22. El tipo y la escala de las computadoras y las redes correspondientes en los entornos comerciales o gubernamentales pueden ser muy diferentes de los que se observan en los entornos residenciales o de consumidores. A medida que aumenta la adopción de tecnologías de la información y las comunicaciones por la población en general, aparecen nuevos grupos que son más vulnerables a tipos específicos de delitos relacionados con las computadoras, que van desde las infecciones con virus hasta las penetraciones de las computadoras y diversos tipos de fraude contra los consumidores. Cuando los países comienzan a adoptar tecnologías de la información y las comunicaciones, diferentes sectores de la sociedad quedan expuestos a diferentes tipos de delitos relacionados con las computadoras.

IV. Cruce de fronteras: la delincuencia transfronteriza y la ciencia forense informática

23. Cuando se investigan delitos relacionados con las computadoras, hay que hacer frente a numerosos problemas forenses. Parte del problema de reconstruir un incidente en un caso de delito cibernético es que gran parte de las pruebas son intangibles y transitorias. En lugar de pruebas físicas, las investigaciones de delitos cibernéticos procuran encontrar rastros digitales que con frecuencia son inestables y de corta duración. Una de las razones de la inestabilidad es que algunos tipos de información sobre direcciones y rutas electrónicas (es decir, los "datos sobre el tráfico") no se almacenan de manera permanente. Esa información puede quedar sólo en la memoria de un sistema de computadoras por un período corto y luego se le superpone otra ruta de información.

24. Las nuevas tecnologías crean no sólo problemas novedosos, sino también nuevas oportunidades para los investigadores, ya que permiten reconstruir pistas digitales. Hay muchas circunstancias en que los datos sobre el tráfico y otras formas de información sobre gestión de redes se pueden almacenar en registros en lugar de superponerles otra información. En la Internet y en otras redes de computadoras, normalmente se almacena información sobre una variedad de actividades de gestión de redes para su posterior análisis a fin de facilitar la contabilidad de la red, la determinación de la fiabilidad del servicio y del equipo de la red, el historial de fallas, las tendencias del funcionamiento y los pronósticos de la capacidad. Además de estas finalidades, esos datos se pueden utilizar también con fines de comercialización o preparación de perfiles de consumidores (por ejemplo, las consultas a páginas de sitios web de ventas al por menor determinan los productos más populares, las pautas de consumo o los perfiles de los consumidores).

25. Hay, sin embargo, varias consideraciones que determinan si los datos sobre el tráfico o información similar se pueden almacenar. Un factor, por ejemplo, es el tipo de servicio. Un servicio de acceso a una red (por ejemplo, utilizando el protocolo de acceso telefónico de autenticación remota (Remote Authentication Dial-in User Service (RADIUS)), puede almacenar ciertos tipos de información sobre suscriptores y algunos datos sobre tráfico para que los suscriptores puedan tener acceso a la Internet. Esta situación sería más común, en particular, en los servicios que se prestan por tiempo, que deben registrar en qué momento el suscriptor se

conecta y cuánto tiempo permanece en línea. Por el contrario, se reduciría al mínimo en servicios anónimos o que hacen hincapié en la privacidad[22].

26. El correo electrónico, que data de los primeros días de la Internet (estaba disponible en ARPANET en 1971), normalmente contiene información sobre direcciones y otros datos de tráfico en la cabeza de la aplicación[23]. Parte de esa información es creada por el programa cliente del usuario final y otra parte por el servidor de correo electrónico (utilizando el protocolo SMTP (protocolo de transmisión de correo sencillo (Simple Mail Transfer Protocol (SMTP)).

27. El servicio de Internet más familiar probablemente sea la World Wide Web, que en gran parte utiliza el sistema de nombres de dominio (DNS) para establecer la relación entre nombres de dominio (el nombre del lugar de los sitios web) y direcciones del protocolo de Internet (IP) (las direcciones numéricas hacia y desde donde viajan los paquetes). Los servidores de la web pueden almacenar grandes cantidades de datos sobre tráfico relativos a las páginas que se solicitan, y quién (es decir, qué dirección de IP) la solicita. Esa práctica es más común en los servidores comerciales, ya que el registro de los datos puede llegar rápidamente al nivel de gigabytes y, por lo tanto, su almacenamiento puede ser muy costoso.

28. Los servicios de transferencia de ficheros pueden recolectar o no recolectar información de los suscriptores en los registros, según la aplicación. Históricamente, las transferencias de ficheros se realizaban utilizando el protocolo de transferencia de ficheros (FTP), aunque las transferencias en condiciones de seguridad, que están cada vez más cifradas, utilizan el protocolo de conexión segura SSH (Secure Shell). Recientemente, en lugar de los servidores de ficheros centrales, ha surgido el paradigma P2P, que permite a un gran número de usuarios compartir ficheros (recursos descentralizados distribuidos a través de redes de entidades transitorias; como ejemplos se puede citar a Napster, KaZaA, Morpheus, Gnutella y Freenet). Algunas formas de P2P tienen datos sobre tráfico fácilmente accesibles, mientras que otras están diseñadas para evitar el análisis del tráfico.

29. Otros servicios incluyen los aproximadamente 100.000 grupos de noticias de Usenet, que tratan virtualmente todos los temas imaginables. Se accede a ellos mediante una red mundial de servidores de almacenamiento y retransmisión que aplican el protocolo NNTP de transferencia de noticias (Network News Transfer Protocol); algunos datos sobre tráfico pueden estar disponibles en el servidor y otros en las computadoras personales y locales. Hay también muchas formas de conversación en tiempo real, que van desde IRC hasta los mensajes instantáneos.

30. Los diferentes servicios de Internet utilizan por lo general dispositivos de red diferentes (como encaminadores o servidores). Según la configuración del sitio del proveedor del servicio, se pueden almacenar diferentes registros en muchas máquinas diferentes, que pueden estar controladas por diferentes entidades jurídicas y, en algunos casos, situadas en diferentes jurisdicciones.

31. Dada la gama de posibles servicios, diferentes nichos de mercado y una serie de factores que incluyen en el costo del mantenimiento de datos[24], puede decirse que no hay una postura única de las empresas o de la industria sobre la reunión y retención de datos sobre tráfico y datos sobre suscriptores. Es evidente que la retención de ciertos datos de tráfico y de suscriptores puede facilitar a los organismos encargados de hacer cumplir la ley el rastreo de delincuentes en la Internet; algunos países han adoptado recientemente legislación que confiere

carácter obligatorio a la retención de los datos. Aun si no existen leyes que requieran la retención de los datos sobre el tráfico, es crucial que los investigadores forenses comprendan las diversas prácticas de gestión de redes y contabilidad de redes de los proveedores de servicios de Internet para determinar el grado en que las necesidades de los organismos que hacen cumplir las leyes pueden satisfacerse con las prácticas ordinarias de los proveedores de servicios de Internet[25]. La cooperación de estos proveedores puede ser valiosísima cuando las autoridades procuran investigar y enjuiciar delitos cibernéticos.

32. La investigación y el enjuiciamiento efectivos de los delitos relacionados con las computadoras suelen requerir el rastreo de la actividad delictiva a través de una diversidad de proveedores de servicios de Internet o compañías con computadoras conectadas a la Internet. Para lograr el éxito, los investigadores deben seguir la pista de las comunicaciones hasta la fuente y las computadoras u otros dispositivos afectados, trabajando con proveedores de servicios intermedios en diferentes países. Para ubicar la fuente del delito, los organismos de represión suelen basarse en los archivos históricos que muestran cuándo, desde dónde y quién ha hecho las diferentes conexiones. En otros momentos, esos organismos deben seguir la pista de la conexión cuando está activa. Cuando los proveedores están situados fuera de la jurisdicción territorial del investigador, como suele ser el caso, los organismos de represión necesitan ayuda de sus contrapartes de otras jurisdicciones. Las medidas tradicionales de asistencia judicial recíproca, y aun las medidas más expeditivas, están previstas normalmente para obtener datos históricos y en tiempo real de casos en que están involucrados sólo dos países (por ejemplo, el país de la víctima y el país del delincuente). Cuando el delincuente encamina comunicaciones a través de tres, cuatro o cinco países, el proceso de asistencia judicial requiere períodos sucesivos antes de que los organismos de represión puedan obtener datos de cada uno de los proveedores de servicios en la etapa siguiente de la pista de las comunicaciones, con lo que aumenta la posibilidad de que los datos no estén disponibles o se hayan perdido, y de que el delincuente permanezca encubierto y en libertad para cometer nuevos actos delictivos[26].

33. A fin de prestar asistencia en las investigaciones de delitos relacionados con las computadoras, el Subgrupo sobre delitos de alta tecnología del Grupo de los Ocho comenzó a preparar en 1997 un sistema de contactos permanentes para los delitos internacionales relacionados con las computadoras y de alta tecnología, una lista de delitos cibernéticos que está a disposición de los organismos de represión 24 horas al día, los siete días de la semana (sobre una base “24/7”). La red de contacto, que actualmente incluye a 40 países, también forma parte de la Convención sobre el Delito Cibernético del Consejo de Europa, que ofrece un conjunto de instrumentos de investigación para combatir todos los delitos cometidos contra un sistema de computadoras o mediante el uso de uno de esos sistemas.

34. Dada la prevalencia de virus, parásitos y piratas que aprovechan las vulnerabilidades de los sistemas, es también necesario contar con mecanismos que permitan responder con rapidez. En docenas de países de todo el mundo se han establecido Equipos de Respuesta para Emergencias Informáticas (CERT). Sus funciones principales son:

a) Proporcionar un panorama amplio de los métodos de ataque, las vulnerabilidades y los efectos de los ataques sobre los sistemas y las redes de

información; suministrar información sobre incidentes y características y tendencias de la vulnerabilidad;

b) Crear una infraestructura de profesionales de la seguridad cada vez más competentes, que respondan rápidamente a los ataques contra sistemas conectados a la Internet y estén en condiciones de proteger sus sistemas contra amenazas a la seguridad;

c) Proporcionar métodos para evaluar, mejorar y mantener la seguridad y la supervivencia de los sistemas de redes;

d) Trabajar con los vendedores para mejorar la seguridad de los productos como fueron despachados[27].

35. Si el perpetrador puede estar en un país, el ataque lanzarse desde computadoras situadas en otro país y los efectos sentirse en un tercer país, es evidente que, además de la inestabilidad de los datos, hay problemas jurídicos que tienen que ver con las fronteras y las jurisdicciones. La investigación y el enjuiciamiento de delitos relacionados con las computadoras destacan la importancia de la asistencia judicial recíproca. Con todo, las cuestiones de soberanía son sólo uno de los problemas que se plantean en situaciones de registro e incautación. Sin una asistencia judicial recíproca apropiada se corre el riesgo de que los funcionarios de los organismos de represión de un Estado efectúen búsquedas de información transfronterizas no autorizadas en computadoras situadas en otro Estado. Aun antes de considerar siquiera la asistencia judicial recíproca, sin embargo, es necesario reflexionar sobre la legislación nacional. Después de todo, la cooperación internacional requiere en definitiva que los países cuenten con leyes capaces de hacer frente a los delitos cibernéticos.

V. La legislación nacional: condición indispensable

36. En algunos casos, ciertos tipos de delitos cibernéticos se esparcen como epidemias que ignoran las fronteras nacionales. En otros casos, los elementos del delito se escurren a través de las fronteras mediante una estrategia cuidadosa y premeditada de confusión y desorientación. El aumento de la densidad de las tecnologías de la información y las comunicaciones para aprovechar los beneficios de la sociedad de la información aumenta también la frecuencia de los delitos cibernéticos internos. Por lo tanto, interesa desde el punto de vista económico y de la seguridad pública que los países promulguen leyes nacionales para combatir los delitos relacionados con las computadoras.

37. Las leyes nacionales han evolucionado a través de los siglos, mientras que la Internet se ha desarrollado en sólo unas pocas décadas. Por supuesto, las leyes se siguen adaptando a los cambios en la sociedad. En respuesta a los desafíos que plantean los delitos cibernéticos, las legislaciones nacionales quizá deban modernizarse. Sieber ofrece un relato de seis ondas principales de legislación sobre delitos cibernéticos que los países han adoptado desde el decenio de 1970[28]: a) protección de datos y protección de la privacidad; b) el derecho penal trata los delitos económicos relacionados con las computadoras; c) protección de la propiedad intelectual; d) protección contra el contenido ilícito y nocivo; e) derecho

procesal penal; y f) normas jurídicas sobre medidas de seguridad como la criptografía y las firmas digitales[29].

38. Se necesitan varios elementos para hacer frente a la delincuencia relacionada con las computadoras: a) asegurar que los delitos estén definidos en la ley; b) establecer poderes de investigación legales para combatir los delitos cibernéticos; y c) realizar estas actividades de manera que ofrezcan salvaguardias que protejan los derechos humanos y las libertades fundamentales.

A. Delitos sustantivos

39. Se han desarrollado listas bastante completas de delitos contra la confidencialidad, la integridad y la disponibilidad de sistemas de computadoras[30]. Hay también varios delitos relacionados con el contenido (como la producción y distribución de pornografía infantil o material xenofóbico) incluidos en la clase de delitos relacionados con las computadoras.

> La Oficina de Supervisión de la Seguridad de la Información del Ministerio de Seguridad Pública de China informó que en 2001 se habían denunciado poco menos de 5000 delitos cibernéticos, en comparación con 2900 en 2000 y unos 400 en 1999. A mediados de 2002, la Oficina había comunicado poco más de 3000 casos, y se estimaba que al final de 2002 se habrían denunciado 350 casos de penetración de sistemas y más de 800 casos de daños a sistemas de computadoras[31]. El número de casos identificados por la Oficina crecía a una tasa abrumadora, y muchos casos no se comunicaban o pasaban desapercibidos. La mayoría de los infractores eran jóvenes (de 18 a 30 años de edad) y la mayoría de los ataques se iniciaban en cafés cibernéticos o de redes, en los que los infractores ocultaban su identidad conectándose a través de un protocolo de transferencia de hipertexto (HTTP) o un sustituto (*Sock proxy*), utilizando direcciones de IP falsas o empleando criptografía o esteganografía. En consecuencia, China había adoptado enérgicas medidas para registrar y vigilar los cafés cibernéticos.

40. Se plantearon numerosas cuestiones cuando los países intentaron adoptar disposiciones diseñadas para bienes físicos y utilizarlas en el mundo intangible y efímero de los bienes digitales.

41. Cuando se formulan disposiciones, hay que tener cuidado de evitar la penalización de acciones que pueden ser legítimas. Cuando se actualiza una ley penal, hay una línea muy estrecha que divide lo específico de lo general. Es posible que las disposiciones redactadas en términos específicos lleguen a ser obsoletas cuando aparezcan nuevas tecnologías. Por consiguiente, es conveniente utilizar un lenguaje “tecnológicamente neutro”.

B. Poderes procesales

42. En los últimos años, debido a la mayor prevalencia de los registros electrónicos, muchos países han debido abordar cuestiones relativas a la definición del término "documentos". Aun términos básicos, como el concepto de "lugar" en que se realiza una búsqueda, pueden plantear problemas jurídicos cuando los datos se distribuyen a través de una red de computadoras (es decir, la búsqueda puede realizarse en una computadora en una oficina en un lugar pero los datos pueden estar almacenados en una computadora situada en otro lugar físico, aunque "virtualmente" accesible para el usuario y el investigador).

43. Cuando se elaboran facultades procesales, es conveniente distinguir entre tres clases diferentes de información: a) el contenido real de las comunicaciones electrónicas; b) los datos sobre tráfico; y c) la información sobre los suscriptores. Esto puede ser conveniente porque estos tres tipos de información pueden tener expectativas diferentes de privacidad o protección de los datos, o pueden afectar a otros derechos humanos y libertades fundamentales.

44. Uno de los primeros retos jurídicos que se plantean es establecer una definición de "datos sobre el tráfico" y "información sobre el suscriptor". La Convención sobre los Delitos Cibernéticos del Consejo de Europa[32], por ejemplo, define los datos sobre el tráfico como "todo dato de computadora relativo a una comunicación por medio de un sistema de computadoras, generado por un sistema de computadoras que forma parte de una cadena de comunicación, y que indica el origen de la comunicación, el destino, la ruta, la hora, la fecha, el tamaño, la duración o el tipo de servicio subyacente" (artículo 1). La Convención define la información sobre el suscriptor como "toda información, contenida en forma de datos de computadora o en cualquier otra forma, en posesión de un proveedor de servicios, relativa a los suscriptores de sus servicios, distinta de los datos sobre el tráfico o sobre el contenido, mediante la cual se puede determinar:

"a. El tipo del servicio de comunicaciones utilizado, las disposiciones técnicas adoptadas y el período del servicio;

"b. La identidad del suscriptor, su dirección postal o geográfica, el número de teléfono y otros números de acceso, información sobre facturas y pagos, disponible sobre la base del acuerdo o arreglo de servicios;

"c. Toda otra información sobre el sitio en que está instalado el equipo de comunicaciones, disponible sobre la base del acuerdo o arreglo de servicios (párrafo 3 del artículo 18)."

45. La cuestión de las definiciones se considera en el Manual de las Naciones Unidas sobre prevención y control de delitos informáticos[33] y también se trata en la decisión marco del Consejo de la Unión Europea sobre ataques contra sistemas de información, así como en leyes nacionales[34].

46. En la legislación nacional de muchos países, ciertos tipos de contenido pueden estar sujetos a una mayor protección constitucional en virtud de conceptos como "comunicación privada" y "libertad de expresión". Es pues necesario distinguir, jurídica y procesalmente, entre el contenido de ciertas clases de comunicaciones por la Internet (aquellas que no son públicas sino privadas) y los datos sobre el tráfico. También es posible que ciertos elementos de los datos sobre el tráfico y la

información sobre los suscriptores[35] puedan, en ciertos contextos, estar vinculados a disposiciones sobre protección de datos porque constituyen información bibliográfica básica que puede estar sujeta a la protección de la privacidad.

47. Cabe señalar que la reunión de datos y su posterior retención están cargadas de intereses y valores en conflicto de los diversos interesados directos, y puede que sea conveniente establecer un equilibrio entre los diversos intereses legítimos. En algunas jurisdicciones, la reunión de datos está estrictamente limitada por las prácticas de información justas, a veces consagradas en leyes sobre privacidad o protección de datos, en virtud de las cuales sólo se puede reunir datos para fines limitados, y los datos se pueden utilizar sólo para una finalidad declarada, con consentimiento fundamentado, y sujetos a otras salvaguardias de uso (como las comprobaciones de la integridad de la información, los calendarios de eliminación conocidos y los sujetos del acceso)[36].

48. Las tecnologías de almacenamiento y retransmisión suelen dar lugar a cuestiones jurídicas singulares en las jurisdicciones que tienen diferentes regímenes jurídicos para vigilar el contenido en tiempo real (como las disposiciones sobre captación de las comunicaciones telefónicas), a diferencia de la búsqueda e incautación. Con respecto a los delitos relacionados con las computadoras, ésta puede ser una cuestión relativa al correo electrónico que puede requerir una autorización para vigilar el contenido en tiempo real cuando un mensaje de correo electrónico está en tránsito, pero puede requerir un mandamiento de registro e incautación cuando está detenido (es decir, almacenado en un servidor de correo electrónico o en el disco duro del usuario final). En la medida en que el mensaje es esencialmente el mismo en ambas circunstancias, se plantean preocupaciones en razón de que hay recurso a dos instrumentos jurídicos diferentes, con dos umbrales jurídicos potencialmente diferentes.

49. Se han desarrollado varios instrumentos jurídicos para facilitar las investigaciones relacionadas con las computadoras, incluidos los mandamientos de preservación y los mandamientos de presentación. El mandamiento de preservación es un mecanismo expeditivo que dispone que los proveedores de servicios almacenen y resguarden los datos existentes que son específicos de una transacción o de un cliente. Ese mecanismo de procedimiento es importante en el contexto de las pruebas electrónicas, dado que éstas pueden ser borradas o destruidas con más facilidad que los documentos físicos. Esencialmente, un mandamiento de preservación es una orden de “no borrar”. El mandamiento de preservación[37] es de naturaleza temporaria y se expide para que los organismos de represión tengan la autoridad legal necesaria para obtener los datos (como un mandamiento para incautar datos o un mandamiento de presentación para que se liberen los datos).

50. Un mandamiento de presentación exige al custodio de los documentos que los entregue o que los ponga a disposición de los organismos de represión dentro de un plazo determinado. Los mandamientos de presentación son similares a los mandamientos de registro, aunque en el caso de un mandamiento de presentación el custodio de los documentos es quien realiza la búsqueda, y no la policía. Este tipo de mandamientos crea menos problemas, ya que el custodio suele estar en mejores condiciones para conocer con exactitud la ubicación de los documentos de que se trata. En el entorno comercial de la actualidad, es común que las corporaciones almacenen datos fueran de la jurisdicción en la que operan, con frecuencia para aprovechar los menores costos del almacenamiento de datos. Un mandamiento de

registro tradicional puede no ser apropiado en esas circunstancias, mientras que los mandamientos de presentación permiten al dueño de los datos o al custodio recuperar los documentos o los registros.

VI. Soluciones basadas en la cooperación internacional

51. Puede que sea necesario adaptar las leyes nacionales para incluir los delitos cibernéticos a fin de responder con eficacia a las peticiones de asistencia de otros Estados o para obtener la asistencia de éstos. La compatibilidad con las leyes de los otros Estados es un objetivo importante que se debe tener en cuenta cuando se elabora legislación sobre delitos relacionados con las computadoras. A fin de respetar los derechos soberanos de los Estados y facilitar la cooperación internacional, es necesario estudiar la posibilidad de ofrecer mecanismos internacionales formales, como las convenciones. Para que la asistencia judicial recíproca funcione efectivamente, los delitos sustantivos y los poderes procesales de una jurisdicción deben ser compatibles con los de la otra.

52. La comunidad internacional apenas está comenzando a enfrentar los múltiples desafíos que siguen apareciendo en este campo. Un ataque masivo de denegación de servicio que utilice cientos de computadoras comprometidas de varios países para atacar sitios web comerciales en otro país, o el daño considerable causado por un virus o parásito que abarca a dos tercios del mundo plantean problemas fundamentales, por ejemplo, dónde se ha cometido el delito y a quién hay que enjuiciar. Otra cuestión fundamental es si las medidas eficaces dependerán en última instancia de cuál Estado podría tener la capacidad y la voluntad de comprometerse a realizar la investigación e iniciar actuaciones penales. Es evidente que los delincuentes cibernéticos transnacionales están preparados para explotar las lagunas creadas por las diferencias de los marcos jurídicos y de la capacidad de los sistemas de justicia penal. Habrá quienes consideren que esto socava la soberanía, mientras que otros pueden sostener que el mundo es testigo de la transformación de la soberanía que se produce a medida que las sociedades de la información comienzan a emerger en el mundo.

53. Esos escenarios rápidamente ponen de relieve la compleja cuestión de la extradición, que en sí misma puede dar lugar a numerosos problemas. Por ejemplo, a falta de una compatibilidad funcional de los delitos sustantivos, la definición del delito puede ser tal que no sea posible cumplir el requisito de la doble incriminación. Al mismo tiempo, se acepta cada vez más que cuando se requiere la doble incriminación, son las conductas subyacentes o los elementos básicos del delito los que deben corresponder, y no solamente la forma en que se tipificó el delito en los países de que se trate. Aun cuando la doble incriminación no plantea un problema en un caso específico, el tipo de delito relacionado con las computadoras puede no ser considerado de gravedad suficiente (por ejemplo, en términos de las disposiciones sobre sentencia) para que haya lugar a la extradición.

54. Pese a estos problemas, sin embargo, se han logrado varios éxitos importantes desde 2000, cuando se celebró el décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente, incluidos dos nuevos instrumentos jurídicos: la Convención contra el Delito Cibernético del Consejo de Europa y la Convención de las Naciones Unidas contra la Delincuencia Organizada

Transnacional, que es de ámbito global pero trata indirectamente de los delitos cibernéticos cuando los cometen grupos de delincuentes organizados.

55. En el plano internacional, la función de entidades como la Oficina de las Naciones Unidas contra la Droga y el Delito (ONUDD), la Organización Internacional de Policía Criminal (Interpol), la Organización de Cooperación y Desarrollo Económicos (OCDE), y el Grupo de los Ocho, así como órganos regionales como la Unión Europea, el Consejo de Europa, la Organización de los Estados Americanos, la Asociación de Naciones del Asia Sudoriental, y la Cooperación Económica de Asia y el Pacífico (APEC) proporcionan la experiencia política y técnica necesaria para fomentar la cooperación internacional. A diferencia de unos años atrás, ahora es posible hablar de un consenso internacional para combatir los delitos cibernéticos, especialmente las formas trasnacionales que se dan con frecuencia. Por consiguiente, hay finalmente un "clima moral" para una acción concertada, ya sean medidas civiles, penales o administrativas, y esta cooperación reconoce lo que los sociólogos denominan "comunidades de destinos compartidos"[38].

56. La Convención sobre el Delito Cibernético se abrió a la firma el 23 de noviembre de 2001 y ha sido firmada por 30 Estados y ratificada por 8 Estados. (La Convención puede ser firmada por Estados de fuera de Europa y ya la han firmado cuatro Estados no europeos (Canadá, los Estados Unidos, Japón y Sudáfrica).) La convención entró en vigor el 1 de julio del 2004. Requiere que los Estados partes armonicen las leyes nacionales que definen los delitos sustantivos. Éstos incluyen los delitos contra la confidencialidad, integridad y disponibilidad de datos y sistemas de computadoras, así como los delitos relacionados con las computadoras como la falsificación y el fraude cibernético, los delitos relacionados con la infracción de los derechos de autor, y los delitos de pornografía infantil cometidos utilizando un sistema de computadoras. Además, la Convención prevé un conjunto importante de poderes procesales, incluidos los mandamientos de presentación y los mandamientos de preservación, diseñados para facilitar las investigaciones y los enjuiciamientos en el contexto de las redes de computadoras mundiales. Hay también disposiciones para establecer un sistema rápido y eficaz de cooperación internacional. Por último, la cuestión de los "delitos motivados por prejuicios" en la Internet dio lugar a un protocolo adicional de la Convención sobre el Delito Cibernético para penalizar actos de naturaleza racista o xenofóbica cometidos mediante sistemas de computadoras[39], que se abrió a la firma el 28 de enero del 2003. El protocolo adicional ha sido firmado por 20 Estados y ratificado por dos.

57. En 2002, los Ministros de Justicia del Commonweallth aprobaron una Ley Modelo denominada Ley sobre delitos contra sistemas de computadoras y relacionados con las computadoras[40]. La Ley Modelo, que comparte un marco común con la Convención sobre el Delito Cibernético, proporciona a los organismos de represión instrumentos eficaces y modernos para combatir la delincuencia cibernética. Los fiscales, los investigadores y los legisladores pueden evaluar los materiales desarrollados en el plano internacional, como las directrices, los manuales jurídicos y técnicos, las prácticas recomendadas y la legislación modelo para ayudar a sus autoridades a establecer leyes nacionales.

58. A partir del octavo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente, celebrado en 1990, las Naciones Unidas han participado activamente en el estudio de diversos aspectos de los conceptos

relacionados con las computadoras[41]. En 1994, se publicó el Manual de las Naciones Unidas sobre prevención y control de delitos informáticos[42], con asistencia financiera y sustantiva considerable del Gobierno del Canadá y expertos aportados por otros gobiernos y organizaciones no gubernamentales.

59. En 2000, durante el décimo Congreso, se celebró un seminario sobre delitos relacionados con las redes de computadoras[43]. En 2001, el Secretario General presentó a la Comisión de Prevención del Delito y Justicia Penal las conclusiones de un estudio sobre medidas eficaces para prevenir y combatir los delitos relacionados con las computadoras y de alta tecnología (E/CN.15/2001/4).

60. En 2004, como uno de los resultados de la primera etapa de la Cumbre Mundial sobre la Sociedad de la Información, celebrada en Ginebra en diciembre de 2003, el Secretario General estableció el Grupo de Trabajo sobre la gobernanza de la Internet encargado de estudiar las cuestiones de la inundación de mensajes (*spam*), la seguridad cibernética y otras cuestiones relacionadas con la Internet en preparación de la segunda etapa de la Cumbre Mundial, que se celebrará en Túnez en noviembre del 2005.

61. La delincuencia relacionada con las computadoras es un fenómeno internacional que requiere una solución también internacional. Para lograr esa solución, la comunidad internacional debe examinar cuidadosamente los medios que ya tiene a su disposición para fortalecer la cooperación internacional. Debe tratar también de aumentar sus conocimientos y su comprensión de las diversas manifestaciones del fenómeno, los desafíos que plantean esas manifestaciones y la viabilidad y los medios convenientes para prevenir y combatir el fenómeno.

VII. La cooperación en las investigaciones sobre la delincuencia relacionada con las computadoras

62. La tarea de proporcionar una base de pruebas para la futura evolución de la política constituye un desafío. Las investigaciones sobre la delincuencia relacionada con las computadoras está en su infancia. Es posible que los individuos y las instituciones con conocimientos, tanto del sector público como del sector privado, sean renuentes, por razones de orden comercial, político o de seguridad nacional, a compartir sus conocimientos con los investigadores. La información que llega al dominio público suele ser incompleta o imprecisa. Pese a estos inconvenientes, es importante desarrollar una base de conocimientos, a fin de que empiecen a tener efecto las actividades para eliminar la brecha digital.

63. Hay que utilizar una variedad de métodos de investigación y criterios comparativos para proporcionar datos básicos sobre la prevalencia y gravedad de los diversos tipos de delitos cibernéticos. También son fundamentales las investigaciones sobre la efectividad de las nuevas leyes, estrategias de policía y enjuiciamiento mediante exámenes de casos y estudios de desgaste. Las investigaciones no se deben limitar a los datos de la policía o los tribunales, y esas fuentes con frecuencia deben ser más específicas y uniformes. Las esferas que requieren investigación con más urgencia incluyen el comportamiento de la víctima y el infractor, así como el seguimiento de las novedades en materia legislativa y de aplicación de la ley en todo el mundo[44].

VIII. La cooperación del sector público y el sector privado en la lucha contra la delincuencia relacionada con las computadoras

64. Cada vez con más frecuencia, los gobiernos y los representantes del sector privado reconocen la necesidad crítica de una colaboración estrecha en sus actividades para combatir la delincuencia relacionada con las computadoras. Ningún gobierno o grupo de gobiernos y ninguna empresa o el sector industrial pueden lograr el éxito actuando separadamente; en cambio, tiene que haber una estrecha colaboración de los sectores público y privado, definida por la apertura y por un sistema de comunicaciones firmes en las dos direcciones. Las entidades de los sectores público y privado han cumplido y continuarán cumpliendo una función esencial en el desarrollo de tecnologías para ayudar a prevenir e investigar los delitos cibernéticos. No obstante, aparte de encontrar soluciones tecnológicas, el sector privado puede también cumplir la importante función de ayudar a los entes normativos a determinar prioridades legislativas y soluciones. La experiencia ha mostrado que una asociación activa entre el gobierno y la industria puede facilitar actividades de represión más eficaces contra los delincuentes cibernéticos.

65. Es alentador que se estén multiplicando las asociaciones entre los sectores público y privado. Los Miembros del Grupo de los Ocho reconocieron hace mucho tiempo que una respuesta eficaz contra los delitos cibernéticos exige una cooperación sin precedentes entre el gobierno y la industria, y han adoptado importantes medidas en ese sentido, incluida la organización de conferencias para representantes gubernamentales y de la industria, a fin de examinar preocupaciones comunes y posibles soluciones[45]. Las Naciones Unidas, los países de la APEC, la OCDE y otras organizaciones multilaterales también están poniendo más empeño en obtener la participación del sector privado en esas actividades.

66. En diciembre de 2004, representantes de diversas industrias y organismos de represión internacionales anunciaron el establecimiento de Digital PhishNet, una operación de colaboración que reúne a líderes industriales en los campos de la tecnología, la banca, los servicios financieros y las subastas en línea con los organismos de represión para atacar el problema del "*phishing*", una forma destructiva y creciente de robo de identidad en línea. Digital PhishNet establece una línea de comunicación única y unificada entre la industria y los organismos de represión, a fin de que se puedan compilar datos esenciales para combatir la pesca de información ("*phishing*") y proporcionarlos a los organismos de represión en tiempo real. Aunque otros grupos industriales han hecho hincapié en la identificación de los sitios web de pesca de información y el intercambio de las mejores prácticas e información sobre casos, Digital PhishNet es el primer grupo de su clase que concentra su atención en ayudar a los organismos encargados de hacer cumplir las leyes penales y colaborar en la detención y el enjuiciamiento de los responsables de delitos de "pesca" contra los consumidores. Digital PhishNet reúne a líderes de la industria de 9 de los 10 principales bancos y proveedores de servicios financieros de los Estados Unidos, cuatro de los cinco principales proveedores de servicios de la Internet y cinco empresas de tecnología y comercio digital, y trabaja con los principales organismos de represión federales e internacionales.

67. Durante los últimos años, varias entidades el sector privado se han unido a la Universidad de Hong Kong para celebrar varias conferencias importantes sobre la delincuencia cibernética. Esos acontecimientos reunieron a oficiales superiores de justicia y organismos encargados de hacer cumplir la ley de Asia y el pacífico, así como a importantes académicos y representantes de las organizaciones multilaterales principales, incluidas las Naciones Unidas, el Consejo de Europa, la Interpol y la APEC. Los temas de debate incluyeron los desafíos a la seguridad de las redes, las amenazas al comercio electrónico que plantean la inundación de mensajes, la "pesca" y otras formas de fraude en línea, y la piratería en línea.

68. Los oficiales de represión de todo el mundo han trabajado en los últimos años junto con varias empresas bien conocidas, para investigar y enjuiciar a los autores de fraude en línea y otros delincuentes cibernéticos, incluidos algunos de los "*spammers*" más conocidos del mundo.

69. Pese a estos progresos, se puede hacer más para aumentar el nivel de colaboración entre los gobiernos y la industria y proporcionar una mayor estructura y regularidad al diálogo y las asociaciones de entidades de los sectores público y privado.

IX. Recomendaciones

70. El 11º Congreso quizá desee considerar las siguientes recomendaciones formuladas en dos reuniones de expertos, de las que fue anfitrión del Instituto Coreano de Criminología en Seúl, teniendo tener en cuenta también las recomendaciones pertinentes de las reuniones preparatorias regionales del 11º Congreso:

a) Es preciso tratar los problemas de la delincuencia cibernética en un marco de inclusión y amplio, más allá del derecho penal, los procesos penales y las actividades de represión. Este marco debe incluir los requisitos para el funcionamiento en condiciones de seguridad de una economía cibernética, optimizando la confianza en los negocios y la privacidad individual, así como estrategias para promover y proteger las innovaciones y el potencial de creación de riqueza y oportunidades de las tecnologías de la información y la computación, incluidos los mecanismos de alerta temprana y de respuesta en caso de ataques cibernéticos. En el trasfondo de la prevención y el enjuiciamiento de los delitos relacionados con las computadoras se vislumbra el desafío más grande de crear una cultura mundial de la seguridad cibernética, atendiendo a las necesidades de todas las sociedades, incluidos los países en desarrollo, que tienen estructuras de tecnología de la información emergentes y todavía vulnerables;

b) Se debe seguir desarrollando la cooperación internacional a todos los niveles. En razón de su carácter universal, el sistema de las Naciones Unidas, con los mecanismos de coordinación interna mejorados que ha pedido la Asamblea General, debe asumir el liderazgo de las actividades intergubernamentales para asegurar el funcionamiento y la protección del ciberespacio a fin de impedir que no sea objeto de abuso o explotación por los delincuentes o terroristas. En particular, el sistema de las Naciones Unidas debe ser el instrumento para promover enfoques mundiales de la lucha contra la delincuencia cibernética y los procedimientos de cooperación internacional, con miras a impedir o mitigar los efectos negativos de

este tipo de delincuencia sobre la infraestructura crítica, el desarrollo sostenible, la protección de la privacidad, el comercio electrónico, las operaciones bancarias y el comercio;

c) Se debe alentar a todos los Estados a que pongan al día sus leyes penales lo antes posible, a fin de tener en cuenta la naturaleza particular de la delincuencia cibernética. Con respecto a las formas tradicionales de delitos cometidos mediante el uso de las nuevas tecnologías, esta actualización puede hacerse aclarando o aboliendo disposiciones que ya no son completamente adecuadas, como las leyes que no abarcan la destrucción o el robo de intangibles, o creando nuevas disposiciones para nuevos delitos, como el acceso no autorizado a computadoras y redes de computadoras. Esa actualización debe incluir a leyes procesales (por ejemplo, para seguir la pista de las comunicaciones) y a las leyes, acuerdos o arreglos de asistencia judicial recíproca (por ejemplo, para la rápida preservación de los datos). Al determinar la rigurosidad de la nueva legislación, se debe alentar a los Estados a que se guíen por las disposiciones de la Convención sobre el Delito Cibernético del Consejo de Europa;

d) Los gobiernos, el sector privado y las organizaciones no gubernamentales deben colaborar para eliminar la brecha digital, elevar la toma de conciencia por la población sobre los riesgos de la delincuencia cibernética y aplicar contramedidas apropiadas y mejorar la capacidad de los profesionales de la justicia penal, incluido el personal de los organismos de represión, los fiscales y los jueces. A tal fin, las administraciones de justicia nacionales y las instituciones de enseñanza del derecho deben incluir en sus planes de estudio programas amplios sobre delitos relacionados con las computadoras;

e) El 11º Congreso debe prestar mucha atención al establecimiento, la mejora y la ampliación de los instrumentos prácticos actuales, para el intercambio internacional de información, la alerta temprana y los mecanismos de respuesta, las medidas para limitar el daño en la lucha contra la delincuencia cibernética (utilizando a la Interpol, los mecanismos de alerta 24/7 del Grupo de los Ocho, la Convención sobre la Delincuencia Cibernética, los Equipos de Respuesta para Emergencias Informáticas (CERT) y el Foro de Respuesta a Incidentes y Equipos de Seguridad (FIRST)), que por el momento existen sólo en algunos países, en su mayoría desarrollados. Estos instrumentos deben estar a disposición de la comunidad internacional a fin de que se puedan compartir los conocimientos y la información sobre los medios de reconocer, proteger, evitar y combatir nuevos tipos de delitos cibernéticos e informar a la población acerca de los mecanismos de respuesta eficaces. Además, se debe prestar especial atención a velar por que estos instrumentos prácticos estén a disposición de los países en desarrollo y ofrecer a estos países la capacitación necesaria;

f) La política sobre delincuencia cibernética debe basarse en las pruebas y estar sujeta a una evaluación rigurosa para asegurar su eficiencia y eficacia. Por lo tanto, se deben realizar actividades concertadas y coordinadas a nivel internacional para establecer mecanismos de financiación con el fin de facilitar las investigaciones prácticas y poner freno a muchos tipos de los nuevos delitos cibernéticos emergentes. No obstante, es igualmente importante asegurar que las investigaciones estén coordinadas a nivel internacional y que sus resultados reciban la más amplia difusión posible;

g) La ONUDD debe someter a la consideración de la Cumbre Mundial sobre la Sociedad de la Información en su segunda etapa, que se celebrará en Túnez en 2005, los resultados del Seminario sobre medidas para combatir los delitos relacionados con las computadoras.

Notas

[1] D. B. Parker, S. Nycum y S. S. Oüra, *Computer Abuse* (Menlo Park, California, Stanford Research Institute, 1973).

[2] Donn B. Parker, *Computer Crime: Criminal Justice Research Manual* (Washington, D.C., Departamento de Justicia de los Estados Unidos, 1979).

[3] Donn B. Parker, *Computer Crime: Criminal Justice Research Manual* (Washington, D.C., Departamento de Justicia de los Estados Unidos, 1989).

[4] Russell G. Smith, Peter N. Grabosky y Gregor F. Urbas, *Cyber Criminals on Trial* (Cambridge, Cambridge University Press, 2004).

[5] Consejo de Europa, *European Treaty Series*, No. 185.

[6] En algunos países en que los usuarios residenciales de la Internet han adoptado las LAN inalámbricas, se han utilizado LAN inseguras para obtener acceso no autorizado a la Internet para diversos fines. Esto se ha vinculado con frencuencia a la "conducción de guerra" ("*war driving*") (el uso de una computadora portátil en un automóvil para ubicar y registrar puntos de acceso o "*hot points*").

[7] En algunos países, el concepto de "robo" se refiere sólo a bienes tangibles y comprende privar a una persona de una cosa tangible; por lo tanto, no abarca el robo de un bien intangible y no abarcaría la obtención de una copia de un fichero digital. Algunos países no aplican a esas acciones sanciones penales, pero en cambio las someten al derecho civil, incluidos los regímenes de derechos de autor.

[8] El programa informático de Bram Cohen "BitTorrent peer-to-peer" se utiliza cada vez más para compartir grandes ficheros de datos para fines legítimos (como la distribución de programas de fuente abierta, juegos de computadoras o el envío a usuarios múltiples de programas de televisión ("*peer-casting*")) y la piratería de vídeos. Véase en Clive Thompson, "The Bit Torrent effect", *Wired*, 13 de enero de 2005; y Jeff Howe, "The shadow Internet", *Wired*, 13 de enero de 2005, una sinópsis de la piratería de vídeos.

[9] *IC3 2003 Internet Fraud Report*: *January 1, 2003-December 31, 2003* (National White Collar Crime Center y Oficina Federal de Investigaciones de los Estados Unidos).

[10] Véase Michael D. Mehta, Don Best y Nancy Poon, "Peer-to-peer sharing on the Internet: an analysis of how Gnutella networks are used to distribute pornographic material". *Canadian Journal of Law and Technology*, vol. 1, No. 1 (enero de 2002); y Estados Unidos de América, Oficina de Contaduría General, *File Sharing Programs: Peer-to-peer Networks Provide Ready Access to Child Pornography*, GAO-03-351 (Washington, D.C., febrero de 2003).

[11] Dick Thornburgh y Herbert S. Lin, eds., *Youth, Pornography and the Internet* (Washington, D.C., National Academy Press, 2003).

[12] Véase una sinópsis de las leyes de 24 países relativas a los materiales racistas, xenofóbicos y antisemíticos en el documento sobre el tema examinado por la Conferencia sobre el antisemitismo de la Organización para la Seguridad y la Cooperación en Europa (CIO.GAL/25/04/Rev.1), celebrada en Berlín el 28 y 29 de abril de 2004.

[13] Scott Berinato, "The truth about cyberterrorism", *CIO Magazine*, 15 de marzo de 2002.

[14] Respecto de los productos comerciales disponibles que utilizan criptografía cuántica para cifrar datos en sistemas con base de fibra óptica o redes inalámbricas, véase Gary Stix, "Best-kept secrets", *Scientific American*, enero de 2005.

[15] Véase un análisis de los aspectos de tecnología de la información y las telecomunicaciones de los objetivos de desarrollo del Milenio en: Unión Internacional de Telecomunicaciones, *World Telecommunication Development Report 2003: Access Indicators for the Information Society*, 7th ed. (2003). El estudio ofrece una interesante evaluación de los objetivos de desarrollo del Milenio pertinentes a las tecnologías de la información y las comunicaciones; el nuevo índice de acceso digital (Digital Access Index (DAI)) parece especialmente prometedor.

[16] China Internet Network Information Center, *15th Statistical Survey Report on the Internet Development in China (Jan. 2005)* (www.cnnic.net.cn) (consultado el 25 de enero de 2005).

[17] Internet Systems Consortium (http://www.isc.org).

[18] Derivado de Unión Internacional de Telecomunicaciones, *World Telecommunication Indicators Database*, 8a. ed. (2004).

[19] *Estudio Económico y Social, 2000* (publicación de las Naciones Unidas, No. de venta S.00.II.C.1).

[20] Véase un análisis estadístico de la complejidad de la brecha digital en el marco conceptual propuesto en George Sciadas, ed., *Monitoring the Digital Divide ... and Beyond* (2003).

[21] Se ha señalado que, irónicamente, estas circunstancias reproducen en un plano diferente la brecha digital precisamente en un momento en que estaba a punto de ser eliminada y puede llegar a socavar la confianza de las empresas locales o el incipiente atractivo para las inversiones.

[22] La diferencia principal entre un servicio anónimo y un servicio de seudónimos es que este último preserva una identidad (un "alias" o "*nym*") durante un cierto período (y, por consiguiente, puede haber un enlace más fuerte entre la identidad del seudónimo, la identidad del suscriptor y la identidad en el "mundo real"). Un servicio anónimo, en su forma más pura, es esencialmente un servicio de una sola vez o de transacción única. Hay diversos tipos de servicios anónimos y de seudónimo; la mayoría provee sustitutos, cadenas o redes mixtas de acceso a uno o más servicios comunes de Internet como reexpedidores de mensajes, navegación en la web, IRC o grupos de noticias de Usenet. Hay también grados de anonimidad o pseudo anonimidad, que no depende simplemente de factores como el cifrado subyacente y el programa de autenticación sino también de la naturaleza y seguridad de servidor de anonimidad o la red de servidores, los procedimientos de creación de "*nym*" y, en el caso de los servicios de pagos, el mecanismo de facturación.

[23] David H. Crocker, rev., *Standard for the Format of ARPA Internet Text Messages*, RFC 822 (13 de agosto de 1982).

[24] En el seminario sobre retención de datos celebrado durante el Diálogo gobierno/industria sobre seguridad y confianza en el ciberespacio del Grupo de los Ocho, celebrado en Berlín en octubre de 2000, se determinaron las siguientes consecuencias financieras para la retención de datos: volúmenes de depósitos de registros; recuperación de datos pertinentes; ingeniería y desarrollo; gastos administrativos, operacionales y de capacitación; provisión de seguridad y privacidad; responsabilidad por la manipulación y entrega a organismos de represión; y gastos relacionados con la oportunidad y la confianza del cliente.

[25] Los datos pueden permanecer en manos de los proveedores por diferentes períodos, según los modelos comerciales, los servicios y las tecnologías. Algunos datos se mantienen con fines de facturación, otros para los sistemas de auditoría de la ejecución. Los períodos varían desde unos pocos segundos hasta períodos más largos que puedan ser necesarios o permitidos, para fines distintos de la aplicación de las leyes, por sus legislaciones nacionales. Los diferentes tipos de datos sobre tráfico también se mantienen por diferentes períodos; por ejemplo, los registros de

acceso a las redes (RADIUS o TACACS+ (acceso específico para la autentificación y autorización en servidores) tienen diferentes necesidades comerciales y de almacenamiento de datos que los registros NNTP y, en consecuencia, en ciertas circunstancias pueden estar disponibles por períodos más largos. El contenido normalmente no se retiene ni está disponible.

[26] *Recommendations for Tracing Networked Communications across National Borders in Terrorist and Criminal Investigations* (http://canada.justice.gc.ca/en/news/g8/doc2.html).

[27] Véase *CERT Coordination Center, 2003 Annual Report* (www.cert.org); y Foro de Respuesta a Incidentes y Equipos de Seguridad (www.first.org).

[28] Ulrich Sieber, *Legal Aspects of Computer-Related Crime in the Information Society: COMCRIME Study* (1 de enero de 1998).

[29] El modelo de Sieber de seis ondas de legislaciones nacionales se ha aplicado a la experiencia australiana en Russell G. Smith, Peter N. Grabosky y Gregor F. Urbas, *Cyber Criminals on Trial* (Cambridge, Cambridge University Press, 2004).

[30] Organización de Cooperación y Desarrollo Económicos, *Computer-Related Crime: Analysis of Legal Policy*, ICCP Series, No. 10 (1986); véase también la recomendación No. R (89) 9, aprobada por el Comité de Ministros del Consejo de Europa el 13 de septiembre de 1989.

[31] Informe de país para China, proporcionado para la Conferencia de Asia y el Pacífico sobre el Delito Cibernético y la Seguridad de la Información, celebrada en Seúl del 11 al 13 de noviembre de 2002 por la Comisión Económica y Social para Asia y el Pacífico y el Ministerio de Información y Comunicaciones de la República de Corea. El número de infractores puede ser grande debido a que, en un distrito de Beijing (Protectorado del Distrito de Haidian), entre 2001 y mayo de 2004 se arrestó a 52 sospechosos, el 48,4% de ellos por piratería.

[32] Consejo de Europa, *European Treaty Series*, No. 185.

[33] *Revista Internacional de Política Criminal*, Nos. 43 y 44 (publicación de las Naciones Unidas, No. de venta S.94.IV.5).

[34] La Ley de reglamentación de los poderes de investigación de 2000 del Reino Unido tiene una definición de datos de tráfico en su artículo 2.9, aunque esa definición incluye también la información sobre el suscriptor. Hay un concepto de datos de tráfico en las definiciones de los Estados Unidos de "*pen register*"y "*trap and trace device*" (Código de los Estados Unidos, título 18, artículo 3127) que fue actualizada en la Ley de unión y fortalecimiento de América proporcionando los instrumentos adecuados que se requieren para inteceptar y obstruir el terrorismo (PATRIOT Act) de 2001.

[35] Con respecto a la información sobre el suscriptor, puede que en algunos países ya haya una reglamentación en el campo de la telefonía (información sobre el nombre y la dirección del cliente.)

[36] Entre los instrumentos internacionales pertinentes figuran, por ejemplo, el Convenio sobre la protección de las personas en relación con el proceso automático de datos del Consejo de Europa (Consejo de Europa, *European Treaty Series*, No. 108) o las Directrices de la Organización de Cooperación y Desarrollo Económicos (OCDE) sobre la protección de la privacidad y las corrientes transfronterizas de datos personales, de 1980. Esos instrumentos procuraron establecer principios según los cuales la información personal se debe obtener de buena fe; usar sólo para los fines originales especificados; debe ser adecuada, pertinente y no excesiva para ese fin; precisa y actualizada; accesible al sujeto; mantenida en condiciones de seguridad; y destruida una vez utilizada. La obligación se reforzó en algunas jurisdicciones, por ejemplo, mediante las directivas sobre protección de datos del Parlamento Europeo y el Consejo de la Unión Europea (directiva 95/46/EC y directiva 97/66/EC). A partir de esos instrumentos, numeros países de Europa han promulgado leyes aún más rigurosas de protección de los datos para cumplir sus obligaciones jurídicas de aplicar los estándares de las directivas. Fuera de Europa, también hay instrumentos con disposiciones similares relativas a los datos personales,

como la Ley de documentación electrónica y protección de la información personal del Canadá.

37 Cabe señalar que “la “preservación de datos” asegura que la información especificada existente en relación con un suscriptor determinado no sea borrada. Por otro lado, la “retención de datos” es un requisito general diseñado para obligar a todos los proveedores de servicios de Internet a reunir y retener una serie de datos relativos a todos los sucriptores.

38 Roderic Broadhurst, “Content crimes: criminality and censorship in Asia”, monografía presentada en Octopus Interface: the Challenge of Cybercrime, Estrasburgo, Francia, 15 a 17 de septiembre de 2004.

39 Consejo de Europa, *European Treaty Series*, No. 189.

40 La ley modelo se puede consultar en las páginas de la División de Asuntos Jurídicos y Constituciones de la Secretaría del Commonwealth en la web http://www.thecommonwealth.org/shared_asp_files/ uploadedfiles/{DA109CD2-5204-4FAB-AA77-86970A639B05}_Computer%20Crime.pdf).

41 Durante el octavo Congreso, se celebró un seminario sobre la computadorización de la administración de justicia penal (A/CONF.144/14). Ya en 1992, la Organización produjo la *Guía para la informatización de los sistemas de información en materia de justicia penal* (publicación de las Naciones Unidas, No. de venta S.92.XVII.6). Durante el noveno Congreso sobre Prevención del Delito y Tratamiento del Delincuente, en 1995, se celebró un seminario sobre la cooperación y asistencia internacionales en la administración del sistema de justicia penal: la computadorización de las operaciones de justicia penal y el desarrollo, análisis y uso de la información sobre justicia plenal (A/CONF.169/13) (véase también Instituto de las Naciones Unidas de Asia y el Lejano Oriente para la Prevención del Delito y el Tratamiento del Delincuente, *The Global Challenge of High-Tech Crime: Workshop on Crimes related to the Computer Network; Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, 15 April 2000, Vienna, Austria* (Tokio, abril de 2001)).

42 *Revista Internacional de Política Criminal*, Nos. 43 y 44 (publicación de las Naciones Unidas, No. de venta S.94.IV.5).

43 Véase el documento de antecedentes para el seminario sobre delitos relacionados con la red de computadoras (A/CONF.187/10).

44 Peter Grabosky y Roderic Broadhurst, “The future of cyber-crime in Asia”, *Cybercrime: the Challenge in Asia*, Roderic Broadhurst y Peter Grabosky, eds. (Hong Kong University Press, 2005), págs. 347 a 360.

45 Véase “G8 Berlin Meeting: Government/Industry Dialogue on Safety and Confidence in Cyberspace (Summary and Assessment)” (se puede consultar en http://www.mofa.go.jp/policy/economy/summit/2000/lyon.html); y Kuriko Miyake, “G8 concludes Tokyo high-tech crime meeting” (se puede consultar en http://archives.cnn.com/2001/TECH/internet/05/31/g8.cyber.crime.idg).