Naciones Unidas A/CONF.187/10

Décimo
Congreso de las Naciones Unidas
sobre Prevención del Delito y
Tratamiento del Delincuente

Viena, 10 a 17 de abril de 2000

Distr. general
3 de febrero de 2000
Español
Original: inglés

Tema 5 del programa provisional*
Prevención eficaz del delito: adaptación a las nuevas situaciones

Delitos relacionados con las redes informáticas

Documento de antecedentes para el curso práctico sobre delitos relacionados con las redes informáticas

Resumen

Para combatir y prevenir eficazmente los delitos cibernéticos es necesario un enfoque internacional coordinado a diferentes niveles. A nivel nacional, la investigación de esos delitos requiere personal, conocimientos especializados y procedimientos adecuados. Se alienta a los Estados a que consideren la posibilidad de crear mecanismos que permitan obtener oportunamente datos exactos de los sistemas y redes informáticos cuando estos datos se requieran como prueba en procedimientos judiciales. A nivel internacional, la investigación eficaz de los delitos cibernéticos requiere una actuación oportuna, facilitada por la coordinación entre los organismos nacionales de aplicación de la ley y la institución de la autoridad legal pertinente.

En el presente documento, que se suma a las iniciativas internacionales ya adoptadas y las apoya, se examinan los medios para el intercambio de conocimientos especializados técnicos y forenses entre las autoridades nacionales encargadas de aplicar la ley, así como la necesidad de celebrar deliberaciones internacionales acerca de las medidas jurídicas actuales y futuras para fomentar la cooperación en la investigación de los delitos cibernéticos.

* A/CONF.187/1.

V.99-90957

Índice

I. Antecedentes legislativos

1. La Asamblea General, en su resolución 52/91 de 12 de diciembre de 1997, decidió que uno de los cuatro cursos prácticos que se celebrarían en el marco del Décimo Congreso de las Naciones Unidas sobre Prevención del Delito y Tratamiento del Delincuente versaría sobre el tema de los delitos relacionados con la red informática. La Asamblea, en su resolución 53/110 de 9 de diciembre de 1998, hizo suyo el programa de trabajo del Décimo Congreso, que incluía cuatro cursos prácticos de carácter técnico, uno de ellos referente a los delitos relacionados con la red informática. En esa misma resolución, la Asamblea subrayó la importancia de los cursos prácticos e invitó a los Estados Miembros, las organizaciones no gubernamentales y otras entidades pertinentes a que apoyaran los preparativos de los cursos prácticos en los planos financiero, de organización y técnico, incluida la elaboración y distribución de documentación de antecedentes conexa.

2. En su resolución 54/125, de 17 de diciembre de 1999, la Asamblea alentó a los Estados Miembros, a otras entidades interesadas y al Secretario General a aunar esfuerzos para garantizar que los cuatro cursos prácticos que se realizarían durante el Décimo Congreso se centraran claramente en los respectivos temas y lograran resultados prácticos e invitó a los gobiernos interesados a que los complementaran con proyectos o actividades de cooperación técnica concretos. En respuesta a esa resolución, el Instituto de Asia y el Lejano Oriente para la Prevención del Delito y el Tratamiento del Delincuente organizó dos reuniones de expertos sobre delitos relacionados con las redes informáticas, en las que se realizaron la mayoría de los preparativos sustantivos para el curso práctico sobre delitos informáticos. El Centro para la Prevención Internacional del Delito agradece los esfuerzos del Instituto de Asia y el Lejano Oriente para la Prevención del Delito y el Tratamiento del Delincuente y del grupo de expertos, que hicieron posible la celebración de este curso práctico.

II. Objetivo y finalidad del documento de antecedentes

3. La aparición de redes internacionales informáticas, como Internet, permite a los usuarios entablar comunicaciones, actividades y transacciones con otros usuarios de todo el mundo. Dado que las computadoras y las redes pueden ser objeto a la vez de uso legítimo y de uso ilícito, se impone la conclusión de que entre quienes exploran las oportunidades del nuevo medio hay personas y grupos impulsados por motivos delictivos. La lucha contra la delincuencia en el actual entorno de redes informáticas internacionales se complica debido a tres causas principales:

a) El comportamiento delictivo puede producirse en un entorno electrónico. La investigación de los delitos cibernéticos, es decir, de cualquier delito cometido en una red electrónica, exige conocimientos técnicos especializados, procedimientos de investigación y facultades legales de que tal vez carezcan las autoridades encargadas de hacer cumplir la ley del Estado interesado;

b) Las redes informáticas internacionales, como Internet, son medios abiertos que permiten que los usuarios actúen más allá de las fronteras del Estado en el que están situadas. Pero la labor investigadora de las autoridades encargadas de hacer cumplir la ley deben circunscribirse en general al territorio de su propio Estado. Esto significa que, la lucha contra la delincuencia en las redes de computadoras abiertas requiere una intensificación de la cooperación internacional;

c) Las estructuras abiertas de las redes informáticas internacionales ofrecen a los usuarios la oportunidad de elegir el entorno jurídico que mejor se ajuste a sus propósitos. Los usuarios pueden elegir un país en el que determinadas formas de comportamiento que puedan desarrollarse en un entorno electrónico no se hayan tipificado como delitos. Esto puede atraer la actividad de personas de otros Estados en cuyos ordenamientos jurídicos esas mismas actividades constituyan un delito. La existencia de "paraísos informáticos" -Estados que no dan prioridad a la reducción o prevención del uso ilícito de las redes de computadoras, o donde no se han elaborado leyes de procedimiento eficaces- puede obstaculizar los esfuerzos de otros países por combatir los delitos relacionados con las redes de computadoras.

4. El examen que figura a continuación se centra en la manera de lograr una acción internacional coordinada para facilitar, mejorar y perfeccionar los actuales métodos de lucha contra la delincuencia cibernética. Reviste particular interés el papel que pueden desempeñar las Naciones Unidas u otras organizaciones internacionales. Se proporciona información general acerca del curso práctico sobre delitos relacionados con las redes informáticas.

5. Además, se esbozan los tipos de delito previstos con respecto a las redes electrónicas internacionales y se

exploran las razones por las cuales esos delitos requieren una atención y esfuerzos combinados internacionales. La definición de tales delitos debería facilitar una interpretación internacional común y orientar las políticas penales nacionales en esa esfera.

III. Categorías de delitos cibernéticos

6. Las expresiones "sistemas informáticos" o "redes informáticas" utilizadas en el presente documento denotan el entorno electrónico en general. Si bien todavía existen sistemas autónomos, lo corriente es que uno o más sistemas de computadoras, incluidas computadoras personales, se interconecten para formar una red. No se hace distinción entre redes públicas y privadas, ni basada en el hecho de que tengan conexiones permanentes. A los efectos del presente documento y salvo indicación en contrario, los sistemas de telecomunicaciones se agrupan en la misma categoría que los sistemas y las redes informáticos.

7. En la actualidad, Internet es un ejemplo bien conocido de red informática pública que ha tenido un crecimiento explosivo en el último decenio. Debe gran parte de su éxito a la utilización de protocolos de comunicación comunes. Cualquier operador de sistema o de red que aplique esos protocolos puede convertirse fácilmente en un eslabón con la función de "proveedor", y recibe en el presente documento la denominación de proveedor de servicios de Internet. Por razones técnicas y comerciales, los proveedores de servicios de Internet de algunos países se organizan en asociaciones o sociedades, que asumen posiciones comunes sobre determinados temas[1]. Se estima que actualmente más de 200 millones de personas utilizan Internet en todo el mundo, 112 millones de ellas en América del Norte, 47 millones en Europa y 33 millones en la región de Asia y el Pacífico[2]. Al fin de 1995 existían, según las estadísticas, 26 millones de usuarios, la mayoría de los cuales residían en los Estados Unidos de América. En 1999, el aumento mensual del número de usuarios se estimaba en más de un 3%.

8. La función principal de un sistema informático es el procesamiento de datos. El término datos se define como informaciones, instrucciones o conceptos representados de manera convencional en una forma adecuada para el entendimiento humano o el procesamiento automático[3]. Los datos electrónicos se representan mediante una sucesión de marcas magnéticas en un medio de almacenamiento permanente o temporario, o en forma de cargas eléctricas, cuando se transfieren. Cuando los datos pueden ser identificados y controlados por un portador de datos determinado, como sucede con los almacenados en (un conjunto de) discos flexibles, pueden considerarse, desde el punto de vista jurídico, un objeto material tangible. En general, los datos procesados en un sistema informático ya no pueden modificarse ni controlarse por medio de su portador. Los sistemas operativos transfieren de manera autónoma archivos de datos de un lugar físico en un medio de almacenamiento a otro. En las redes informáticas, el procesamiento de los datos distribuidos hace que sea imposible para quienes controlan los datos determinar la ubicación física de la totalidad o una parte de un archivo sin la adopción de medidas específicas. Los datos como tales sólo pueden controlarse mediante operaciones lógicas y no mediante actos físicos, por lo que resulta difícil tratarlos en estado puro, en el ámbito legal, como si fueran objetos tangibles.

9. Por delito cibernético se entiende todo delito que puede cometerse por medio de un sistema o una red informáticos, en un sistema o una red informáticos o contra un sistema o una red informáticos. En principio, el concepto abarca todo delito que puede cometerse en un medio electrónico. En el presente documento, la palabra "delitos" denota formas de comportamiento generalmente definidas como ilegales o que probablemente serán declaradas ilegales en breve plazo. Es posible que determinada conducta se tipifique como delito en un Estado y no en otros, pero como se explica en el párrafo 13, en ciertos foros internacionales se ha llegado a una identidad de opiniones sobre el un entendimiento común en cuanto al tipo de comportamiento relacionado con los sistemas y redes informáticos que debe declararse ilegal. Éste es el punto de partida del análisis que figura a continuación.

10. La atención se centra en la investigación y el enjuiciamiento penal de los delitos cibernéticos. La denominación "autoridades encargadas de aplicar la ley" denota las autoridades a las que la ley encomienda la investigación y el enjuiciamiento de los actos delictivos. Algunos Estados Miembros han establecido dependencias especializadas para investigar los delitos relacionados con computadoras o prestar asistencia en esas investigaciones. En el plano internacional, la Organización Internacional de Policía Criminal (Interpol) es la que coordina el registro y la distribución de información policial relativa a cuestiones tales como personas buscadas y bienes robados.

11. Al investigar los delitos cibernéticos, las autoridades encargadas de aplicar la ley de un Estado pueden tratar de

obtener la cooperación de autoridades de otros Estados tanto en forma de asistencia en casos concretos como de intercambio de información sobre organizaciones y casos delictivos. Pueden, en el curso de determinada investigación, solicitar la utilización de materiales disponibles en otros Estados. El alcance de la cooperación entre las autoridades nacionales encargadas de aplicar la ley viene determinado por el derecho interno de cada Estado, así como por acuerdos internacionales, incluidos acuerdos de asistencia judicial recíproca.

12. Como ejemplos comunes de uso indebido de redes informáticas internacionales cabe citar la comunicación de expresiones prohibidas por la ley, los ofrecimientos de productos ilícitos o las falsas ofertas con miras a obtener beneficios financieros ilegales. En estos casos, Internet se usa de la misma manera que cualquier otro instrumento o herramienta que pueda utilizarse para cometer un delito. La propia red es el medio en que se perpetra el delito, y no un elemento indispensable para su comisión. Las características específicas de Internet pueden inducir al autor a utilizarla en lugar de los medios tradicionales: ofrece excelentes facilidades de comunicación y la posibilidad de ocultar la propia identidad, y el riesgo de ser objeto de investigación penal en cualquiera de las jurisdicciones involucradas es relativamente bajo. Además de las formas de delincuencia mencionadas, algunos usuarios de Internet obtienen acceso ilegal a sistemas conectados, interfiriendo con su funcionamiento o contenido. Esta actividad se denominó "delincuencia informática". Los autores de delitos informáticos se sirven de su competencia técnica, de conocimientos especializados o de instrumentos específicos para llevar a cabo sus actividades ilícitas. Los sistemas informáticos pueden ser blancos fáciles si no se han incorporado o adoptado las medidas de seguridad correspondientes, o si los usuarios ignoran los riesgos que corren. Además, los factores que facilitan la utilización de un programa tienden a convertirlo en poco seguro. A menudo son de conocimiento público las fallas de seguridad de programas informáticos para sistemas de computadoras que tienen éxito desde el punto de vista comercial.

13. Si bien los países interesados han examinado los problemas planteados por la delincuencia cibernética transnacional, no se ha prestado a este tema demasiada atención, a nivel mundial. Las Naciones Unidas, por ejemplo, aún no han adoptado una política concreta para penalizar los delitos cibernéticos; las leyes nacionales, si se aplican a los delitos cibernéticos lo hacen de diversas maneras. Entre las razones de la falta de importancia dada a la delincuencia cibernética cabe señalar los niveles relativamente bajos de participación en las comunicaciones electrónicas internacionales, la escasa experiencia en materia de aplicación de la ley y los pocos daños que se prevé causarán a la sociedad los delitos electrónicos. En el caso de las redes informáticas mundiales, la política penal de un Estado tiene una influencia directa en la comunidad internacional. Los delincuentes cibernéticos pueden encauzar sus actividades electrónicas a través de un determinado Estado en el que ese comportamiento no esté tipificado como delito y por lo tanto quedar amparados por las leyes de ese país. Incluso si un Estado no tiene un interés nacional especial en tipificar como delito determinado comportamiento, puede considerar la posibilidad de hacerlo a fin de evitar convertirse en un paraíso informático y aislarse internacionalmente. Es esencial la armonización del derecho penal sustantivo en lo concerniente a los delitos cibernéticos si se quiere lograr la cooperación internacional entre las autoridades encargadas de aplicar la ley y las autoridades judiciales de los diferentes Estados.

14. Existen dos subcategorías de delitos cibernéticos:

a) Delito cibernético en sentido estricto ("delito informático"): todo comportamiento ilícito que se valga de operaciones electrónicas para atentar contra la seguridad de los sistemas informáticos y los datos procesados por ellos;

b) Delito cibernético en sentido lato ("delito relacionado con computadoras"): todo comportamiento ilícito realizado por medio de un sistema o una red informáticos, o en relación con ellos; incluidos los delitos como la posesión, el ofrecimiento o la distribución ilegales de información por medio de un sistema o una red informáticos.

15. Según la definición del párrafo anterior, el delito informático está en relación con todo comportamiento ilegal que atente contra la seguridad de sistemas y datos mediante operaciones electrónicas. La seguridad de los sistemas y datos informáticos puede determinarse en función de tres principios: garantía de confidencialidad, integridad o disponibilidad de los datos y funciones de procesamiento. De conformidad con la lista de la Organización de Cooperación y Desarrollo Económicos, de 1985[4] y la Recomendación formulada en 1989[5] por el Consejo de Europa, que es más detallada, los delitos contra la confidencialidad, la integridad o la disponibilidad incluyen:

a) El acceso no autorizado, es decir, el acceso sin derecho a un sistema o una red informáticos violando medidas de seguridad;

b) El daño a los datos o a los programas informáticos, es decir, borrado, la descomposición, el deterioro o la supresión de datos o de programas informáticos sin derecho a ello;

c) El sabotaje informático, es decir, la introducción, la alteración, el borrado o la supresión de datos o de programas informáticos, o la interferencia en sistemas informáticos, con la intención de obstaculizar el funcionamiento de un sistema de computadoras o de telecomunicaciones;

d) La interceptación no autorizada, es decir, la interceptación, realizada sin autorización y por medios técnicos, de comunicaciones destinadas a un sistema o a una red informáticos, provenientes de ese sistema o esa red o efectuadas dentro de dichos sistema y red;

e) El espionaje informático, es decir, la adquisición, la revelación, la transferencia o la utilización de un secreto comercial sin autorización o justificación legítima, con la intención de causar una pérdida económica a la persona que tiene derecho al secreto o de obtener un beneficio ilícito para sí mismo o para una tercera persona.

16. El primer delito, el acceso no autorizado, a veces denominado piratería informática, ocurre con frecuencia y a menudo en combinación con el segundo, el daño a los datos informáticos o con el espionaje informático. Una variante moderna y popular es la piratería dirigida contra un sitio en la *web* para introducir en él información ofensiva o perjudicial. Para investigar eficazmente los delitos de piratería informática se requiere por lo general la cooperación de la víctima y algún medio de sorprender al autor *in fraganti*. Los autores son a menudo jóvenes tecnófilos brillantes que tal vez tengan escasa noción moral de sus actos o de su potencial de daño. Además de los delitos de piratería, algunos países han tipificado como delito actividades como el tráfico de contraseñas o de dispositivos para piratería informática.

17. La descomposición de datos y de programas informáticos incluye el lanzamiento de "gusanos" o virus. Un gusano puede en última instancia paralizar por completo el funcionamiento de la computadora, mientras que un virus puede causar la pérdida de todos los datos almacenados en el disco duro. Una forma moderna de distribuir virus es hacerlo a través de mensajes de correo electrónico no solicitados. Los usuarios de Internet tal vez no tengan conciencia del riesgo inherente a las redes electrónicas abiertas y la recepción de mensajes no solicitados. Es posible que, por razones económicas, no se apliquen los programas de exploración de virus disponibles a nivel comercial. Puede resultar difícil para los investigadores en el ámbito penal probar quién fue el responsable del lanzamiento de un virus que ha causado daños. Los piratas también pueden abusar (temporariamente) de las fallas de seguridad en los programas de sistemas frecuentemente usados y pueden obtener acceso a sistemas informáticos ajenos, o (en casos excepcionales) ejercer control sobre ellos, almacenando funciones específicas de programas en esos sistemas. Los usuarios de Internet tal vez no estén adecuadamente informados o al corriente de los posibles riesgos y las medidas de seguridad adicionales ofrecidas por los fabricantes de programas informáticos.

18. El fraude relacionado con la informática ha sido definido por el Consejo de Europa (véase el párrafo 15 *supra*) como la introducción, la alteración, el borrado o la supresión de datos o de programas informáticos, u otra interferencia en el curso del procesamiento de datos que cause una pérdida económica o de bienes poseídos por otra persona con la intención de obtener una ganancia económica ilícita para sí mismo o para otra persona. Esta disposición se refiere a la situación en que el autor del delito interfiere -con o sin derecho- en el funcionamiento correcto del procesamiento de datos de una computadora con el efecto especificado en la definición de fraude. No abarca las conocidas estratagemas para estafar a las personas urdidas por medio de representaciones o comunicaciones electrónicas a través de Internet, como los ofrecimientos de venta de acciones a precios favorables; las inversiones inmobiliarias en un Estado extranjero; los empréstitos con un tipo de interés excepcionalmente alto; el pago anticipado de artículos descritos con vaguedad; o los incentivos para participar en planes de pirámides. Es probable que las disposiciones tradicionales en materia de fraude se apliquen a esos planes.

19. La falsificación informática definida por el Consejo de Europa (véase el párrafo 15 *supra*) como la introducción, la alteración, el borrado o la supresión de datos o de programas informáticos, u otra interferencia en el curso del procesamiento de datos de manera o en condiciones tales que, conforme a la legislación nacional, constituirían un delito de falsificación si se hubieran cometido con respecto a un objeto tradicional de dicho delito. La finalidad de la norma es tipificar como delito la falsificación de datos informáticos, de manera equivalente

desde el punto de vista funcional a la tipificación como delito de la falsificación de documentos convencionales.

20. Cabe mencionar aquí otros dos tipos de delitos conexos. El primero se refiere a una serie de formas de engaño en relación con los servicios de telecomunicaciones. En esos casos, para obtener servicios sin pagarlos, el autor recurre a la manipulación técnica de determinados dispositivos o de elementos electrónicos de los dispositivos. Esta conducta se tipifica por lo general como delito en normas penales concretas, pero algunas veces puede quedar subsumida en las disposiciones clásicas sobre el fraude o la falsificación. El segundo grupo se relaciona con el uso indebido de instrumentos de pago. Manipulando o falsificando una tarjeta electrónica bancaria, o utilizando códigos falsos, el autor intenta obtener una ganancia financiera ilícita. Tal proceder puede ser objeto de disposiciones penales concretas o de disposiciones clásicas relativas al fraude y a la falsificación, o bien de disposiciones enmendadas en el sentido indicado en el párrafo 19.

21. Los delitos con ayuda de computadora incluyen la puesta a disposición, la comunicación y la difusión de determinado material, y a veces el mero hecho de estar en posesión de ese material. Para cometer estos delitos no se necesitan redes electrónicas; en estos casos las redes son utilizadas por el autor para aumentar el efecto del delito e intentar eludir la justicia. Con respecto a los delitos relacionados con el contenido, conviene distinguir entre un contenido que es ilegal por su carácter o significación y el contenido que no es necesariamente ilegal en sí mismo pero adquiere carácter de tal debido a las circunstancias de su distribución. En esta última categoría entra la violación de los derechos de autor y la venta de bienes o servicios prohibidos como armas, drogas, artículos robados, medicamentos sin receta y acceso a medios de juego. La otra categoría de delitos relacionados con el contenido abarca mensajes difamatorios, que incitan a la subversión o a otras actividades ilícitas, o que son ofensivos debido a su naturaleza discriminatoria en los planos religioso o racial o debido a su naturaleza pornográfica. La medida en que estos comportamientos han sido tipificados como delitos por los legisladores en el plano nacional varía considerablemente. En la mayoría de los casos, los delitos ya estaban previstos desde hacía tiempo en la legislación vigente y la cuestión que se plantea es si las leyes se aplican al nuevo entorno electrónico.

22. Existe acuerdo mundial en las actitudes y normas que condenan la distribución de material pornográfico infantil. Entidades internacionales como la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura y la Unión Europea han recomendado que los países donde la distribución de material de ese tipo todavía no es ilegal promulguen normas penales al respecto. Muchos Estados están preparando o han promulgado leyes contra la pornografía infantil. Las autoridades policiales nacionales e internacionales también conceden alta prioridad a la investigación de esa pornografía.

23. En lo que respecta a los delitos relacionados con materiales que contienen incitaciones al odio o a la discriminación, no existe el mismo grado de consenso general, por diversas razones, en cuanto a si deberían aplicarse leyes penales para castigar la expresión o la distribución. La situación puede cambiar a medida que la comunidad internacional tome conciencia de los efectos negativos de esos comportamientos.

24. La distribución de materiales ilícitos ha originado un debate acerca de la función y las responsabilidades de los proveedores de servicios de Internet. Aparte de algunas iniciativas legislativas para definir y esbozar las obligaciones de precaución de los proveedores, hay una tendencia, tanto en el plano internacional como en el nacional, a asimilar la situación jurídica de esos proveedores a la de los operadores de telecomunicaciones tradicionales. Esto significa que los proveedores de servicios de Internet no tienen por lo general ninguna obligación legal de vigilar o eventualmente bloquear el tráfico que se transmite a través de sus sistemas informáticos. No obstante, por lo general se exige a dichos proveedores que adopten todas las medidas razonables para impedir que continúe la distribución de materiales ilícitos una vez que conocen su naturaleza. También pueden resultar poco claros otros aspectos de la aplicación de las leyes nacionales a los proveedores de servicios de Internet. Como ejemplo cabe citar el alcance de la posible responsabilidad civil por la transmisión de un contenido ilícito, y la medida en que el proveedor está obligado a cooperar con las autoridades encargadas de aplicar la ley proporcionando información para investigaciones penales concretas u otro tipo de asistencia.

IV. La investigación con fines penales de los delitos cibernéticos

25. Como se ha indicado, un delito cibernético puede ser cualquier delito cometido por medios electrónicos o

cometido parcialmente o en su totalidad en un entorno electrónico. Estos delitos se persiguen investigando en dicho entorno. Pero existen otros delitos que también pueden dejar rastros o pruebas en el entorno electrónico. La investigación en entornos electrónicos no se limitará por consiguiente a los delitos cibernéticos en el sentido utilizado en el capítulo anterior, sino que incluirá las indagaciones sobre cualquier delito en cuyo caso sea necesario obtener (posibles) pruebas en un entorno electrónico.

26. Para realizar investigaciones con fines penales en un entorno electrónico, son necesarios conocimientos técnicos especializados, procedimientos adecuados y facultades legales suficientes. El Consejo de Europa, en sus recomendaciones de 1989 y 1995, (R (89) 9 y R (95) 13) subrayó la necesidad de que las autoridades nacionales encargadas de aplicar la ley establecieran dependencias especializadas en delitos informáticos. Estas dependencias deberían dotarse de personal adecuado y de equipos y programas informáticos apropiados. La disponibilidad de personal capacitado y con conocimientos técnicos al día debería asegurarse con programas de capacitación. Muchos Estados ya han creado dependencias de delitos informáticos de ese tipo. Se han preparado diversos manuales con instrucciones técnicas, forenses y de procedimiento sobre la manera de llevar a cabo una investigación para reducir la pérdida de pruebas y garantizan la admisibilidad de éstas ante los tribunales.

27. Algunas dependencias policiales nacionales "patrullan" la Internet, y se han creado programas informáticos específicos para detectar delitos como la piratería informática o la distribución de pornografía infantil. La Unión Europea financió parcialmente la elaboración por la policía sueca de programas informáticos para rastrear el material pornográfico infantil (véase<*http://www.techweb.com*>). Dado el enorme volumen de información que contienen las redes de computadoras internacionales, parece indispensable elaborar programas informáticos como los basados en el reconocimiento de modalidades.

28. Existen dos métodos para obtener datos de un sistema informático, que se basan en criterios técnicos y legales. Conforme al primero, los datos se obtienen como parte de un registro del local o del lugar en el que está ubicado el sistema. El segundo método requiere la interceptación o la vigilancia de los datos transmitidos desde el sistema, hacia él o dentro de él. El presente documento no trata de las facultades legales para efectuar registros de locales. Se supone que dichas facultades legales incluirán competencia para registrar un sistema informático en un lugar determinado. La interceptación puede realizarse por medios técnicos desde el exterior del sistema, o por medio de elementos incorporados al mismo con ese fin.

29. El derecho procesal penal tradicional prevé generalmente la incautación y el bloqueo de sistemas informáticos completos, al igual que en el caso de cualquier otra prueba. Ahora bien, cuando esto no es factible, es posible que se carezca de facultades legales suficientes para investigar el contenido de un sistema computerizado contra la voluntad de su titular o titulares legítimos. La incautación de todo un sistema informático puede resultar técnicamente inviable, o bien ser desproporcionada por tratarse de un entorno con muchos usuarios a los que interesa el contenido de los datos. Cuando se pretende obtener datos para determinadas investigaciones, las facultades legales tradicionales pueden resultar insuficientes a causa de: a) problemas relacionados con la obtención de acceso al sistema informático; b) la naturaleza intangible de los datos; y c) el hecho de que los datos puedan estar almacenados en un sistema conectado, situado fuera del local registrado.

30. Cuando en el local registrado se encuentra un sistema informático, las autoridades encargadas de aplicar la ley están por lo general facultadas para acceder a él e inspeccionar su contenido. Esto será posible si el sistema ya está funcionando, la persona de que se trate lo abre voluntariamente, o se encuentra un medio de acceder a él en el local. Cuando no se da ninguna de estas circunstancias, la cuestión que se plantea es si esas autoridades tienen derecho a acceder al sistema contra la voluntad del individuo en cuestión interesado.

31. Los sistemas, los programas o los archivos de datos informáticos pueden estar protegidos contra el acceso no autorizado. Entonces el acceso se logra generalmente mediante procedimientos de identificación y autenticación conforme a los cuales el usuario presenta una contraseña -en forma manual, incorporada en una tarjeta inteligente, o una combinación de ambas cosas- o debe permitir la verificación de marcas biométricas. Para la seguridad de los datos se suele recurrir al cifrado, que garantiza la autenticación, protege la confidencialidad e implica la utilización de un algoritmo de cifrado y una o más claves. El cifrado plantea el grave riesgo de que, sin la asistencia voluntaria del responsable del sistema o del titular, no se tenga acceso al sistema informático ni a los datos que se buscan. Por lo tanto, algunas leyes exigen que los

responsables permitan el acceso a los sistemas o a los datos, castigando el incumplimiento como desacato a los tribunales. No obstante, esas leyes tal vez no se apliquen cuando el operador de un sistema es también el sospechoso de haber cometido el delito, porque se violarían normas o principios contra la autoincriminación. Además pueden quedar exentas las personas que tengan otras razones legales para no cooperar, como las emparentadas con el sospechoso o las que tengan la obligación profesional de guardar secretos. En algunos casos, si no hay nadie presente a quien pueda exigirse asistencia, puede ordenarse a cualquier otra persona (por lo general un experto externo) que preste esa asistencia. El mero hecho de permitir el acceso a los datos tal vez no sea suficiente si éstos están cifrados. En tales casos, las leyes pueden exigir una mayor cooperación para dar a los datos una forma legible.

32. Los datos como tales son intangibles, de modo que las facultades tradicionales de incautación no les son por lo general aplicables. En el curso de una investigación con fines penales, los objetos tangibles se incautan y trasladan a otra parte, o bien se adoptan medidas para que nadie salvo las autoridades investigadoras pueda disponer de los objetos. En el caso de los datos, basta por lo general con hacer una copia. No obstante, se requieren otras medidas cuando los datos son peligrosos, ilícitos o valiosos, o cuando existe la posibilidad de que las víctimas o la investigación sufran mayores daños. En tales supuestos, las leyes pueden conceder a las autoridades investigadoras la facultad de borar los datos o de impedir su uso posterior. Para proteger los datos, puede resultar necesario copiarlos a fin de restituirlas a su estado original cuando así lo ordene un juez. Si la persona en cuestión protesta contra la copia y posterior utilización de los datos, la ley puede exigir que se levante un atestado sobre los datos incautados.

33. El registro de un sistema informático tendrá lugar por lo general como parte del registro de locales o lugares. La facultad legal de realizar ese registro se ciñe normalmente a los límites físicos del lugar registrado. Una red informática tal vez no esté ubicada en un solo lugar, sino conectada con otras partes de la red mediante líneas de comunicación fijas o con conmutación. En estos casos se plantea la cuestión de si la ley permite registrar los sistemas conectados cuando no estén situados en el lugar en que se realice el registro. Si el registro no es extenso, se corre el riesgo de que los datos sean borrados antes de que se pueda obtener otra orden de registro del lugar en el que estén situados físicamente. En las redes grandes, puede resultar prácticamente imposible establecer la ubicación física exacta de los datos.

34. A continuación se esboza la base legal para facultar a una autoridad para realizar un registro extenso. La persona que reside en el local que va a ser registrado tiene derecho a acceder al sistema informático conectado y a utilizar sus funciones y su capacidad de almacenamiento. Esa persona puede controlar los datos sin necesidad de trasladarse a otra parte. Llegado el momento, la persona está obligada por la ley a someterse al registro de los locales que estén físicamente bajo su control. Cabe argumentar que las mismas reglas serían aplicables a los datos a los que tenga acceso de hecho la persona en cuestión, aunque estén situados en otra parte. La consecuencia sería que el alcance del registro extenso se limitaría a las actividades que dicha persona estuviera autorizada a realizar en relación con el sistema conectado y sus datos, y que no se vulnerarían los derechos de esa persona más de lo permitido con ocasión del registro básico. Sería posible limitar esas facultades a las investigaciones de delitos graves o a los casos en que se requiriera la adopción de medidas inmediatas a fin de impedir la pérdida de pruebas, o bien en ambas circunstancias. Podrían aplicarse otras limitaciones cuando el sistema conectado o los datos objeto del registro estuvieran bajo jurisdicción extranjera (véase el párrafo 59 *infra*).

35. El registro en busca de datos y la selección de éstos en un sistema informático plantea una serie de problemas jurídicos adicionales. El primero de ellos es cuán específica acerca de la naturaleza y el formato de los datos buscados debe ser la orden judicial para que sea legítima. Las leyes nacionales pueden imponer diferentes condiciones restrictivas a este respecto. Además, la ejecución fiel y precisa de la orden judicial puede requerir demasiado tiempo, obligando a las autoridades encargadas de aplicar la ley a hacer una copia de todos los datos que parezcan de interés para su posterior análisis. Las leyes nacionales pueden permitir o no una práctica de esta índole. Otro punto importante es si se debería informar a la persona en cuestión acerca de los datos que se copien y se lleven a otra parte, cuánta información detallada debería proporcionarse y si esa persona deberían tener derecho a impugnar legalmente la incautación. Se plantea además otro problema si los datos son confidenciales o gozan de algún otro tipo de protección legal. La cuestión es cómo identificarlos y protegerlos cuando las autoridades los copian en gran cantidad para su posterior examen.

36. Además, cabe observar que los datos son de naturaleza inestable. Pueden trasladarse, borrarse o alterarse fácilmente sin dejar rastros claros. El procesamiento distribuido de datos no es el único factor de inestabilidad de los datos. El procesamiento electrónico implica el tratamiento de grandes volúmenes de datos de naturaleza efímera que se pueden borrar en cuanto ya no son necesarios. Como ejemplos cabe citar los datos de registro de actividad y los relativos al tráfico de comunicaciones. Si no se tiene conocimiento del conjunto de datos "originales" (si es que este término tiene algún significado en el procesamiento de datos), es difícil detectar manipulaciones y será imposible recuperar los archivos eliminados a menos que se haya mantenido información básica de reserva. La naturaleza de los datos plantea problemas en el caso de los registros físicos:

a) El registro en busca de datos, almacenados o que se estén transfiriendo electrónicamente, debe realizarse en la mayoría de los casos rápida y oportunamente a fin de impedir interferencias en esa búsqueda o alteraciones de los datos;

b) Es necesario adoptar precauciones especiales para que los datos puedan presentarse como prueba ante los tribunales. Su integridad debe quedar asegurada desde el momento en que son extraídos o copiados del sistema informático objeto de registro hasta su utilización ante un tribunal.

37. Las distinciones técnicas y jurídicas entre la incautación de datos almacenados y la interceptación de datos que circulan por la red también se han desdibujado. Los datos se procesan con un sistema informático, llamado a veces dispositivo automático de procesamiento de datos. Esta operación incluye la introducción, la transferencia al equipo periférico (por ejemplo, a la pantalla de vídeo) y los dispositivos intermedios de almacenamiento, el procesamiento propiamente dicho, la transmisión de los resultados a dispositivos periféricos para su almacenamiento y la salida o ulterior transmisión a otros componentes del sistema. La interceptación de datos en un sistema informático se reduce por lo general a la búsqueda de datos almacenados, que ha de realizarse utilizando funciones del sistema o programas informáticos específicos. La búsqueda de datos en transmisión puede realizarse por dispositivos del sistema (vigilancia), si se cuenta con ellos, o bien interceptando técnicamente el flujo de datos en alguna parte de las instalaciones de transmisión. Dado que en muchos casos los datos están tanto almacenados como en transmisión, o pasan frecuentemente de un estado al otro, los investigadores podrán elegir a menudo entre la incautación y la interceptación para obtener los mismos datos. Esto podría plantear problemas jurídicos, porque las normas o salvaguardias que se aplican a la interceptación de las comunicaciones y a la incautación de materiales almacenados no son las mismas en muchos Estados. La interceptación de datos en transmisión está a menudo sujeta a una norma más estricta ya que es una operación encubierta, puede tener por objeto datos que no existían en el momento de autorizarse o de iniciarse la búsqueda y, en la mayoría de los casos, las partes interesadas no tienen conocimiento de la interceptación y tal vez no sean informadas al respecto sino hasta mucho tiempo después de su realización si es que se les da alguna información. El hecho de que los datos de las redes puedan ser tanto incautados como interceptados podría socavar los derechos de los sospechosos en algunos casos, pues permitiría a las autoridades encargadas de aplicar la ley ejercer facultades legales de registro menos restrictivas en algunas operaciones que tuvieran más bien carácter de interceptaciones.

38. Los datos electrónicos, copiados de archivos de datos o registrados de flujos de datos, exigen por lo general precauciones y medidas especiales para que puedan servir de prueba ante los tribunales, si ello es posible en absoluto. En muchos sistemas judiciales, el principio de inmediatez, es decir, que todas las pruebas deben presentarse ante el tribunal, exige que el material probatorio se ajuste a criterios muy elevados. En algunos países pueden existir requisitos de forma que dificulten o impidan la utilización de datos electrónicos como prueba. Algunas leyes exigen que el material esté en forma escrita para que pueda leerse ante el tribunal, por ejemplo. En algunos países, los datos que representan sonidos o imágenes no satisfarían a esta condición y por consiguiente no serían admisibles. Cualquier duda acerca de la fiabilidad del material de prueba determinará asimismo por lo general su inadmisibilidad. Dado que los datos electrónicos pueden modificarse fácilmente sin dejar rastros, ello entraña una pesada carga para las autoridades encargadas de aplicar la ley, que deben reunir esas pruebas de acuerdo con procedimientos transparentes y seguros que les permitan establecer su autenticidad. Para verificar la autenticidad, el tribunal debe estar en condiciones de examinar la fiabilidad del proceso de copia y registro del material de prueba, partiendo del portador original o del canal original de datos. También debe poder comprobar la validez de a) el procedimiento de preservación y la seguridad de la

propia preservación; b) cualquier análisis de ese material; y c) si el material presentado ante el tribunal es conforme al material incautado y guardado originalmente.

39. Además de las facultades convencionales de registrar locales, muchos ordenamientos jurídicos nacionales permiten que los tribunales emitan órdenes de presentación relativas a objetos tangibles. En algunos casos, pueden concederse también facultades paralelas para ordenar la presentación de datos concretos. Estas facultades pueden estar sujetas a restricciones y condiciones específicas que no se aplican a las órdenes de presentación convencionales, para impedir que se ejerzan como medio de obtener información diferente a la especificada. Sin esos controles, por ejemplo, una orden podría obligar a una persona a reunir, procesar o seleccionar cualquier otro tipo de datos que no estén almacenados ni bajo su control. Esta obligación iría más allá del alcance y sentido de una orden de presentación. Al solicitar y utilizar órdenes de presentación, puede resultar útil que las autoridades encargadas de aplicar la ley incluyan los registros de actividad de un sistema informático junto con los demás datos que se desee obtener. Esos registros recogen todas las operaciones realizadas en el sistema en orden cronológico, haciendo constar información sobre puntos como la hora, la duración y los terminales desde los cuales se tuvo acceso a los datos o se introdujeron alteraciones en ellos.

40. De conformidad con las leyes tradicionales de muchos países, es posible que una autoridad judicial o de otra índole ordene la interceptación y grabación de telecomunicaciones en redes públicas. En algunos países se ha ampliado esa facultad para abarcar también redes privadas, nuevas formas concretas de telecomunicación como sistemas móviles y sistemas de telecomunicaciones por satélite y redes de computadoras. La lógica de estas medidas legislativas es que si pueden interceptarse las comunicaciones en una red y no en otra, los delincuentes utilizarán el sistema que presente el menor riesgo de interceptación por parte de las autoridades encargadas de aplicar la ley. La interceptación de determinadas comunicaciones conforme a derecho requiere instalaciones técnicas especiales así como, una base jurídica clara para el montaje de esas instalaciones y la rápida ejecución de una orden judicial de interceptación.

41. A fin de identificar las comunicaciones que han de interceptarse y las personas que sostienen una comunicación interceptada es indispensable contar con la cooperación de los operadores de las redes, como los operadores de telecomunicaciones y los proveedores de servicios de Internet. Sólo estos operadores poseen la información necesaria sobre los abonados. Cuando proceda, la legislación nacional puede imponer a los operadores y proveedores la obligación legal de proporcionar prontamente datos sobre sus abonados si así lo ordenan las autoridades competentes. Una obligaciones legales claras a este respecto protegerían también a las personas y las empresas en materia de responsabilidad civil frente a los abonados.

42. Los operadores de telecomunicaciones y los proveedores de servicios de Internet generalmente poseen datos sobre el tráfico de comunicaciones anteriores, generados por equipo que registra detalles, en particular la hora, la duración y la fecha de cualquier comunicación, las partes que la sostuvieron o el tipo de servicio o actividad. (Nótese el paralelismo con el ejemplo del registro de actividad de un sistema que figura en el párrafo 37 *supra*). Estos datos se conservan por lo general durante un período limitado, según las necesidades comerciales del operador o proveedor y los requisitos legales (en la Unión Europea) o comerciales para la protección de la esfera privada. Muchas leyes nacionales facultan a las autoridades encargadas de aplicar la ley o las autoridades judiciales para ordenar que se reúnan datos sobre el tráfico de futuras comunicaciones. Ahora bien, cuando los datos de tráfico forman parte de la comunicación, como sucede con la "información de encabezamiento" de los mensajes por correo electrónico, la reunión de esos datos de tráfico puede considerarse una interceptación de la comunicación en sí y someterse por ese motivo a restricciones legales. En otros casos, puede considerarse que la reunión de datos sobre tráfico sin interceptar el contenido de la comunicación propiamente dicha es una interferencia menor en la esfera privada de los interesados y someterla por lo tanto a requisitos legales más suaves.

43. Los casos de piratería informática o intromisión electrónica plantean una necesidad particular de rápida interceptación de una comunicación electrónica, así como de pronta disponibilidad de datos sobre tráfico y abonados a fin de descubrir la fuente de la comunicación, preservar los datos y finalmente sorprender al autor *in fraganti* por razones probatorias. De tipificarse como delito, la piratería informática tal vez no sea considerada en algunas legislaciones un delito suficientemente grave como para justificar la aplicación de medidas de interceptación. Generalmente un plan de piratería informática entraña otros actos más graves que pueden determinarse en el momento de detectar las actividades del pirata. Ésta puede

considerarse una razón más para permitir la interceptación en los casos de intromisión electrónica.

44. La interceptación de las comunicaciones electrónicas puede verse obstaculizada por el hecho de que la comunicación esté cifrada. La puesta en cifra se utiliza para permitir la autenticación de un mensaje, identificar al remitente y establecer la integridad de ese mensaje. Una segunda función de la cifra es garantizar la confidencialidad del mensaje (protegiéndolo frente a terceros). En una serie de organizaciones internacionales se han celebrado recientemente deliberaciones sobre posibles políticas criptográficas. Las organizaciones que se interesan por facilitar la aplicación coercitiva de la ley y la lucha contra la delincuencia sienten preocupación por las dificultades para obtener acceso legal a los datos cifrados, mientras que las interesadas por la salvaguardia de la esfera privada y los intereses comerciales son partidarias de la criptografía para proteger la información personal y comercial.

45. Gran parte del debate sobrepasa el alcance del presente documento, pero hay dos cuestiones concretas que conviene examinar aquí. Algunos países productores de medios criptográficos han considerado la posibilidad de controlar la proliferación de esos productos a fin de impedir que grupos delictivos o terroristas consigan acceder a ellos, prescribiendo a tal efecto requisitos de sujeción a licencia de los productos que sean lo suficientemente "resistentes" como para dificultar el acceso de las autoridades encargadas de aplicar la ley. Algunos países también han tratado de aplicar medidas prácticas en un intento de garantizar el acceso legal a las comunicaciones electrónicas protegidas por cifrado. Entre estas medidas figuran la utilización de microplaquetas especiales, sistemas de clave en fideicomiso (en los cuales las claves de los mensajes están bajo la custodia de depositarios fiables a quienes se les pueden incautar legalmente para lograr el acceso) o esfuerzos especiales para el descifrado de mensajes por medios técnicos. Las políticas de esta índole se han enfrentado con algunas dificultades tecnológicas y la oposición de los defensores del derecho a la esfera privada y los intereses comerciales.

46. Es comprensible que garantizar, en el curso de investigaciones penales, el acceso a comunicaciones o datos almacenados cifrados sea un tema que interesa a los organismos encargados de aplicar la ley en todo el mundo. En algunos países ya existen medidas que abordan en parte este problema. En muchos casos los operadores de redes y de telecomunicaciones emplean el cifrado para proteger sus propios sistemas y las comunicaciones de sus clientes. Cuando estos operadores están obligados legalmente a cooperar con las autoridades encargadas de aplicar la ley en la interceptación de determinada comunicación, parece razonable suponer que esa obligación incluye (o podría incluir) el deber de eliminar cualquier cifrado que hubieran aplicado a la comunicación. Pero esto no se extendería al cifrado aplicado directamente por el cliente, que el operador no podría en general descifrar. Otra posibilidad es que los legisladores nacionales consideren la conveniencia de obligar a las personas que participan en una comunicación cifrada a proporcionar los medios de descifrarla cuando así lo ordene la autoridad judicial competente. Como medida protectora entra la autoincriminación, tal orden podría hacerse inaplicable contra los sospechosos u otras personas amparadas por alguna exención legal.

47. Como se señala en el párr. 37 *supra*, la mayoría de los países distinguen entre la interceptación del flujo de datos y la incautación de datos almacenados, pero el correo electrónico representa un desafío a esta distinción porque combina tanto la transferencia como el almacenamiento de datos. Cuando un mensaje se envía es transmitido por el proveedor de servicios del remitente al proveedor de servicios del destinatario. Una vez recibido, este último almacena el mensaje en el buzón del destinatario hasta su apertura. El destinatario tiene acceso al mensaje y determina cuánto tiempo permanecerá en el buzón. Los mensajes del buzón están por consiguiente bajo el control tanto del destinatario como del proveedor y generalmente las autoridades encargadas de aplicar la ley podrían tener acceso ejerciendo medidas coercitivas contra cualquiera de ellos. Normalmente preferirán ejercerlas contra el proveedor de servicios de Internet, dado que de ese modo no alertarían al destinatario sobre la existencia de la investigación. En esos casos, las facultades legales de interceptar una comunicación y efectuar un registro físico del local y de cualesquiera computadoras situadas en él pueden convertirse de hecho en intercambiables. En tal contexto, se podría cuestionar la legalidad de una orden de presentación de los mensajes existentes y de los mensajes que lleguen durante determinado período de tiempo a menos que esa orden de presentación se ajuste a las normas jurídicas (generalmente más estrictas) aplicables a la interceptación. El hecho de que tanto el proveedor como el cliente controlen simultáneamente los datos pueden plantear también interrogantes en cuanto a cuál es la parte cuyos derechos o intereses en materia de esfera privada,

propiedad o de otra índole deben tenerse en cuenta al obtener una autorización legal para llevar a cabo un registro o una interceptación.

V. Cooperación internacional entre las autoridades nacionales encargadas de aplicar la ley

A. Formas de cooperación e iniciativas internacionales

48. Dada la dimensión internacional de las redes electrónicas, es cada vez menos probable que todos los elementos de un delito cibernético se limiten a un solo territorio nacional. En las investigaciones, las autoridades encargadas de aplicar la ley en los diversos Estados necesitarán cooperar a nivel oficial, utilizando mecanismos de asistencia judicial recíproca y estructuras como la Organización Internacional de Policía Criminal (Interpol), y también a nivel extraoficial, proporcionando directamente a las autoridades de otro Estado información de posible utilidad. En general, la cooperación policial internacional presupone el consentimiento de las autoridades de los Estados intervinientes. Según sean las relaciones de los Estados, la naturaleza de la información en cuestión -u otros factores- dicha cooperación también puede requerir un acuerdo internacional en el que se estipulen las autoridades y los procedimientos pertinentes.

49. En 1997, el Grupo de los Ocho, compuesto por los jefes de Estado o de Gobierno del Grupo de los Siete principales países industrializados y de la Federación de Rusia, adoptó una serie de principios jurídicos y un plan de acción común contra a lo que denominó "delincuencia de alta tecnología"[7]. En ellos figuran algunas propuestas relativas a la cooperación práctica entre las autoridades encargadas de aplicar la ley, así como a la elaboración de principios jurídicos relativos a la asistencia judicial recíproca. Entre los elementos de cooperación práctica examinados cabe señalar:

a) Medidas para garantizar la disponibilidad de personal capacitado en número suficiente provisto de la capacidad técnica adecuada, mediante la cooperación en el equipamiento y la capacitación del personal encargado de aplicar la ley;

b) Cooperación en la elaboración de normas forenses para la recuperación y la autenticación de datos electrónicos.

50. A fin de facilitar las respuestas en tiempo oportuno a una solicitud de asistencia presentada por otro Estado, el Grupo de los Ocho convino en establecer un sistema de puntos de contacto, disponibles las 24 horas del día durante los siete días de la semana ("24/7") que ya está funcionando. Las tareas de los puntos de contacto son muy variadas. Cuando así se solicita, un punto de contacto proporciona información fáctica que puede hacer más fácil extender la investigación al otro Estado o apelar a su asistencia, y toma todas las demás medidas necesarias para responder sin demora a una solicitud oficial de asistencia judicial, o bien adopta las medidas preliminares, según lo permita la legislación nacional, en espera de esa solicitud. Los puntos de contacto "24/7" no se limitan al Grupo de los Ocho, sino que se han establecido con carácter voluntario en muchos otros Estados. En algunos países, la creación de unidades especializadas de esa índole tal vez no resulte viable debido a la falta de conocimientos especializados o de medios financieros. En otros Estados, la lucha contra los delitos cibernéticos tal vez tenga menos prioridad. Obviamente, cuanto mayor sea el número de Estados que capaciten y equipen personal y lo mantengan disponible sobre la base de "24/7", mayor será la eficiencia del sistema.

51. En el marco de la Interpol se han establecido varios grupos de trabajo especializados en delincuencia relacionada con a la tecnología de la información. El Grupo de trabajo europeo sobre delincuencia relativa a la tecnología de la información ha elaborado un manual sobre delitos informáticos (disponible en CD-ROM). Contiene instrucciones sobre cómo investigar casos de delincuencia informática, una descripción de los instrumentos y técnicas para la búsqueda y la obtención de material electrónico e información acerca de las leyes sustantivas y de procedimiento pertinentes de diferentes países. Los grupos de trabajo participan activamente en la elaboración de programas informáticos específicos para detectar determinados delitos en Internet. Se han celebrado varios cursos de capacitación para investigadores de delitos informáticos.

52. El Manual de las Naciones Unidas sobre prevención y control de delitos informáticos, tiene por objeto la armonización del derecho procesal y del derecho sustantivo, así como la cooperación internacional en la lucha contra los delitos informáticos. Contiene un capítulo sobre seguridad de la información y la prevención de los delitos cibernéticos[8].

53. Tanto los enfoques coordinados como los que se basan en iniciativas adoptadas por un solo Estado son útiles y es importante maximizar los beneficios de ambos. En este contexto, conviene organizar periódicamente reuniones internacionales para que el personal encargado de combatir los delitos cibernéticos se reúna e intercambie información y experiencias prácticas. Otros mecanismos permanentes como bancos de datos, sitios en la *World Wide Web* y grupos de debate contribuirán a un mejor intercambio de información[9].

54. Un tercer elemento del plan de acción del Grupo de los Ocho es la coordinación de la cooperación entre la industria y el Estado. Ello implica:

a) Alentar a los órganos competentes a que elaboren normas sobre tecnologías de telecomunicaciones y procesamiento de datos fiables y seguras;

b) Desarrollar sistemas de información y telecomunicaciones capaces de detectar el uso indebido de las redes, rastrear a los infractores y reunir las pruebas pertinentes.

Dado que las investigaciones con fines penales en entornos informáticos pueden ser una carga para la industria, la cooperación y coordinación de actividades con la industria es importante y necesaria. Esto engloba múltiples cuestiones, desde la seguridad de la información y la creación de productos hasta la cooperación de hecho en la ejecución de las órdenes judiciales. Las negociaciones entre los gobiernos y las organizaciones industriales pueden adoptar la forma de arreglos sectoriales u otros acuerdos no vinculantes o bien jurídicamente exigibles.

B. Tratados internacionales sobre asistencia jurídica recíproca y otras materias

55. La cooperación internacional en forma de asistencia jurídica recíproca debe basarse en acuerdos internacionales u otros arreglos similares como los de legislación recíproca. Estas disposiciones, tanto multilaterales como bilaterales, obligan a las autoridades de una parte contratante a responder a una solicitud de asistencia jurídica recíproca en los casos convenidos. Esa solicitud sólo se podrá ejecutar si es compatible con el derecho interno del Estado requerido o, en ausencia de normas concretas, en la medida en que no constituya una violación de ese derecho.

56. Los Estados cooperan más eficazmente en cuestiones penales si comparten un interés común, reflejado en leyes o códigos penales recíprocos y en la forma de aplicar el derecho penal en los Estados en cuestión. En muchos convenios internacionales sobre cuestiones penales, el interés común está consagrado en la norma de la doble tipificación penal. Un Estado no puede cooperar con otro en la investigación y el enjuiciamiento de determinados actos si éstos no se penalizan en el Estado requerido. En los convenios ya más antiguos, la falta de la doble tipificación penal es por consiguiente una base válida para denegar la asistencia. En convenios más recientes, no se plantea esta condición formal pero se incluye el criterio del carácter razonable. Es posible que se considere irrazonable atender una solicitud de asistencia judicial si, por ejemplo, el delito en cuestión es de menor cuantía o se relaciona con determinada conducta no tipificada como delito en el Estado requerido.

57. Por lo tanto, una forma de mejorar la cooperación internacional en cuestiones penales es la armonización de determinadas disposiciones sustantivas de derecho penal. Las divergencias culturales, sociales y económicas entre los Estados pueden traducirse en políticas penales diferentes. A este respecto, las deliberaciones internacionales dirigidas a la armonización en materia de delitos relativos a "confidencialidad, integridad y disponibilidad" (véase el párr. 15), por ejemplo para establecer disposiciones orientadas a la tecnología, pueden resultar menos complicadas que las destinadas a la armonización en materia de delitos relacionados con el contenido, debido a las repercusiones sobre los derechos humanos (como la libertad de expresión). La pornografía infantil, respecto de la cual existe un consenso amplio para la aplicación de controles, parece ser la excepción que confirma la regla.

58. La asistencia judicial recíproca significa aquí a cualquier forma de asistencia judicial. Esa asistencia guarda relación generalmente con facultades coercitivas específicas concernientes a la investigación de delitos cibernéticos. Aparte de las solicitudes de asistencia tradicional, como las referidas a las declaraciones de testigos, su finalidad es obtener determinados datos almacenados en un sistema informático situado en el territorio de otro Estado o datos que se están transfiriendo electrónicamente a través de una red y que es posible vigilar o interceptar en el territorio de ese Estado.

59. Los Estados establecen en su derecho interno cuáles de sus facultades pueden aplicarse a la prestación de asistencia a otros Estados signatarios. No tienen por qué poner necesariamente todas sus facultades a disposición de

la investigación de casos penales de otros signatarios. A veces, atendiendo al interés mutuo de los Estados involucrados, puede facilitarse en un caso concreto asistencia que no se prestaría sistemáticamente o habitualmente. La asistencia judicial recíproca, como parte del derecho internacional, se rige también en última instancia por el principio de reciprocidad. Por ésta y otras razones es posible que los Estados que negocian el alcance de la asistencia judicial recíproca con otros Estados vacilen en llegar hasta donde se lo permitiría su derecho interno. La doble tipificación penal -el requisito de que un delito con respecto al cual se solicita asistencia esté tipificado como tal en los dos Estados interesados- también puede invocarse directa o indirectamente como motivo para denegar la asistencia judicial recíproca. Además, los acuerdos internacionales sobre asistencia recíproca pueden contener excepciones en virtud de los cuales ésta no se conceda. Entre las exclusiones más comunes figuran determinados tipos de delito como los fiscales, los políticos o los militares, y los delitos que no se consideran suficientemente graves (en vista de las posibles penas que lleven aparejadas) para merecer el esfuerzo.

60. En la investigación de los delitos cibernéticos internacionales la asistencia judicial puede presentar problemas adicionales. Si una parte no ha previsto en su derecho interno facultades concretas para la búsqueda de pruebas en entornos electrónicos, tal vez no esté en condiciones de responder (o de responder adecuadamente) a una solicitud de asistencia. Por esta razón, la armonización de las facultades coercitivas es una condición importante para la cooperación internacional.

61. También es más probable que la asistencia judicial recíproca revista carácter urgente en los casos de delitos cibernéticos que en los casos de investigaciones convencionales debido a la posibilidad de que las pruebas electrónicas se pierdan si no se obtienen rápidamente. Pero tal vez no siempre puedan adoptarse medidas inmediatas por razones formales y prácticas. Las medidas necesarias pueden requerir una orden judicial en el Estado requerido, por ejemplo. A fin de evitar la pérdida de pruebas en esos casos, podría elaborarse un sistema de medidas preliminares rápidas que requiriesen un mínimo de formalidades, seguido de procedimientos más convencionales una vez obtenidas las pruebas a fin de determinar si deberían remitirse al Estado requirente. Con arreglo a este sistema, la legislación nacional permitiría tanto la obtención de datos en respuesta a una solicitud oficiosa como la preservación de esos datos en espera de la solicitud oficial de revelarlos en el marco del acuerdo de asistencia judicial recíproca. Si esa solicitud no se recibiera a su debido tiempo, o si se denegara por considerarse inadecuada, los datos obtenidos se eliminarían. Es posible aplicar un sistema similar con respecto a la preservación de los datos de tráfico en poder de los operadores de telecomunicaciones o de los proveedores de servicios de Internet.

62. Las redes informáticas internacionales posibilitan la realización en un territorio determinado de actividades que pueden tener (deliberada o involuntariamente) efectos extraterritoriales. Por ejemplo, las autoridades encargadas aplicar la ley de un Estado podrían obtener datos de una red de computadoras como parte de un registro legal en el sector informático en ese Estado, y descubrir luego que algunos de los datos obtenidos han sido almacenados en una parte de la red situada en otro Estado y están protegidos por las leyes de ese Estado. Del mismo modo, un Estado podría interceptar legalmente las comunicaciones electrónicas que pasaran a través de su territorio, aunque esas comunicaciones se realizaran entre personas situadas en otros ámbitos jurisdiccionales donde gozaran de la protección legal de ese Estado contra la interferencia arbitraria en las comunicaciones privadas. También pudiera ser que personas de servicios de aplicación de la ley que operaran en una red actuasen como agentes encubiertos conforme a las leyes de su propia jurisdicción en circunstancias en que sus acciones o los métodos que emplearan contravinieran las leyes de otras jurisdicciones en las que estuvieran operando. Todos estos escenarios son nuevos y sin parangón, y el derecho internacional no proporciona en la actualidad demasiada asistencia u orientación para solucionar las cuestiones que se plantean.

63. Tampoco existe actualmente un consenso amplio acerca de las posibles soluciones a los efectos transfronterizos de las medidas de investigación nacionales aplicadas conforme a derecho. Generalmente se reconoce que un Estado está legalmente autorizado a aplicar medidas de investigación o facultades coercitivas contra cualquiera de sus ciudadanos dentro de su propio territorio, en el cual posee una jurisdicción exclusiva. El ejercicio de esas facultades podría dar por resultado casos de búsqueda y copia de datos, o de posible supresión de éstos, cuando los datos estuvieran situados en otra parte. Desde la perspectiva del Estado objeto del registro, esto puede constituir un acto delictivo conforme a su derecho penal interno y una violación de su soberanía nacional. En cambio, otra opinión es que el derecho internacional no prohíbe una intervención de este tipo porque técnicamente

los datos son accesibles, y se hallan por tanto disponibles desde el Estado que realiza el registro, sin ninguna asistencia o intervención del Estado registrado. Los datos que se hallan en cualquier parte de una red podrían considerarse ubicuos y por esa razón, el acceso a ellos desde cualquier Estado en el que estén presentes sería una cuestión de derecho puramente nacional y no internacional. Desde este punto de vista, no sería necesario involucrar al Estado registrado en ninguna etapa. La medida en que los datos son o no ubicuos (los investigadores deben transferirlos activamente de una jurisdicción a otra, por ejemplo) sigue planteando problemas en derecho internacional.

64. Con respecto a la idea de que toda interferencia en una red de informática situada en el territorio de un Estado representa una violación de la soberanía territorial de ese Estado, conviene tener en cuenta dos opiniones diferentes acerca de la situación del derecho internacional. Una de ellas se basa en el principio de que no debería permitirse a los Estados realizar unilateralmente registros, copias ni ninguna otra interferencia en los datos o los sistemas informáticos situados en otro Estado, por la misma razón que no se les permitiría hacer esas mismas cosas mediante una presencia física unilateral. Para obtener datos de otro Estado a efectos probatorios, deberían seguirse procedimientos establecidos de asistencia judicial recíproca. Esta opinión responde a los principios tradicionales, pero tal vez no es sensible a los problemas prácticos que plantea la investigación de los delitos informáticos.

65. Una opinión más pragmática propugnada por algunos es que el derecho internacional no ofrece actualmente respuestas claras a las cuestiones de violación de las leyes nacionales o conculcación de la soberanía. Los que adoptan esta posición aducen que es posible conformar el derecho internacional mediante la cristalización de un consenso internacional en el sentido de que deberían permitirse esas actividades, y mediante una definición clara de las condiciones en las que se permitirían. Se sugiere como elemento importante de esa solución la notificación al Estado objeto del registro.

66. La comunidad internacional podría presentar nuevos conceptos para establecer una norma jurídica relativa a la definición de los derechos de los Estados en materia de uso compartido de redes informáticas terrestres, móviles o de satélites. Mientras tanto, podría convenirse en un enfoque pragmático que adoptara la forma de un tratado u otro instrumento internacional sobre determinados procedimientos en virtud de los cuales se equilibraran adecuadamente los intereses del Estado que realiza el registro y los intereses del Estado objeto del registro y de su residentes.

VI. Conclusión

67. Debido a la frecuencia creciente de los delitos en el ámbito informático, facilitados por el establecimiento de redes electrónicas internacionales y públicas de alcance mundial, la coordinación y la cooperación internacionales en esta esfera han adquirido una importancia fundamental. Los principales elementos de esa acción internacional podrían basarse en los siguientes principios:

a) *Sensibilización del público en general.* La sensibilización y la educación del público podrían reducir el número de delitos en el entorno electrónico. La industria -fabricantes de equipos y programas informáticos, proveedores de servicios y otros- las organizaciones de consumidores y los gobiernos podrían llevar a cabo una labor común de información pública en materia de seguridad y otros riesgos de los entornos electrónicos abiertos y presentar a la población sugerencias sobre la forma de proteger sus intereses;

b) *Orientación hacia una política común en materia de delitos cibernéticos.* La naturaleza transnacional de los delitos cibernéticos es indicio de que toda estrategia de control debería incluir el desarrollo de políticas comunes sobre las cuestiones esenciales. Estas políticas comunes son importante para impedir la existencia de "paraísos informáticos" en el seno de jurisdicciones donde determinadas actividades no se hayan tipificado como delitos, por ejemplo. La elaboración de políticas comunes podría ser un aspecto del Programa de las Naciones Unidas en materia de prevención del delito y justicia penal, en apoyo de la labor ya emprendida por algunas organizaciones internacionales;

c) *Mejoramiento de las medidas de investigación.* Podrían aplicarse medidas eficaces para mejorar la capacidad de investigación con fines penales en entornos informáticos, especialmente en los casos que afecten a varias jurisdicciones. Esto incluye atender a la necesidad de operaciones que se puedan realizar con rapidez suficiente para prevenir la pérdida o la inaccesibilidad de las pruebas. El registro de los sistemas informáticos y la vigilancia de las redes de computadoras tal vez requieran facultades adicionales que no existen actualmente en el derecho procesal penal tradicional. Los volúmenes de datos existentes en los sistemas informáticos y la facilidad

con la que pueden acceder a ellos los investigadores también plantean importantes problemas relativos a la esfera privada y cuestiones conexas. Los derechos humanos de los interesados deben tenerse en cuenta y sopesarse cuidadosamente, tanto a la hora de crear nuevas facultades legales como a la de ejercerlas.

d) La investigación de los delitos cibernéticos requiere disponer de personal con determinados conocimientos técnicos y forenses especializados y el establecimiento de procedimientos específicos. Esto implica la formulación de programas de capacitación y la elaboración de programas informáticos aptos para la investigación. Deberían prepararse programas internacionales de capacitación y los Estados deberían intercambiar conocimientos especializados. Las Naciones Unidas, en el marco de su Programa en materia de prevención del delito y justicia penal, podrían estudiar la conveniencia de revisar su manual sobre delitos informáticos y seguir apoyando la labor ya iniciada por otras organizaciones internacionales.

e) *Mejoramiento de la coordinación y la asistencia transfronterizas*. Los delitos cibernéticos se cometerán en entornos electrónicos mundiales y no se limitarán necesariamente al territorio de un Estado en particular. Por tanto, es posible que, para su investigación eficaz, los Estados dependan de la asistencia de otros Estados. Ésta incluye tanto la cooperación oficiosa por parte de personal encargado de aplicar la ley como la asistencia judicial recíproca oficial por conducto de las autoridades centrales. La posible inestabilidad de los datos existentes en las redes informáticas hace que la capacidad de proporcionar esa asistencia de una manera rápida y eficaz sea más importante que en el caso de muchos otros delitos. Una asistencia eficaz en los casos de delitos cibernéticos debería basarse en las siguientes medidas:

i) El establecimiento de puntos de contacto similares a los creados por el Grupo de los Ocho a fin de asesorar a los Estados requirentes acerca de la asistencia que puede proporcionarse e iniciar la adopción de las medidas necesarias para satisfacer las solicitudes en la medida en que lo permita el derecho interno;

ii) La revisión de los sistemas de asistencia judicial en el contexto de los delitos cibernéticos. Es necesario proceder a un examen de los requisitos y las prácticas de asistencia judicial convencional para determinar si satisfacen las necesidades de la moderna investigación de los delitos cibernéticos y concretar posibles mejoras. Entre las esferas que podrían examinarse figuran la idoneidad general de las facultades para llevar a cabo investigaciones de tipo penal en entornos informáticos y la posibilidad de adoptar medidas expeditivas a fin de resguardar los datos en beneficio de las investigaciones de tipo penal de otros Estados.

Notas

[1] Algunos ejemplos de asociaciones o sociedades son la Asociación de Proveedores de Servicios de Internet de los Estados Unidos (USIPA), la Asociación Canadiense de Proveedores de Servicios de Internet (CAIP) y la Asociación Paneuropea de Asociaciones de Proveedores de Servicios de Internet de los Países de la Unión Europea (Euro/SPA). En algunos países europeos, por ejemplo en Alemania, Bélgica, España, Francia, Italia, los Países Bajos y el Reino Unido de Gran Bretaña e Irlanda del Norte existen asociaciones nacionales.

[2] *http://www.nua.ie/surveys/how-many-online*, 18 de octubre de 1999.

[3] Véanse las definiciones técnicas de datos de la Organización Internacional de Normalización (ISO).

[4] *Computer-Related Crime*: Analisis of Legal Policy, ICCP Series N° 10; 1986.

[5] Recomendación N° R (89) 9 del Consejo de Europa (1989).

[6] "Global Information Networks: Realising the Potential", Conferencia Ministerial, Bonn, julio de 1997.

[7] Véase el Comunicado de la Reunión de los Ministros de Justicia y de Interior del Grupo de los Ocho, celebrada en Washington, el 9 y 10 de diciembre de 1997, *http://www.usdoj.gov/criminal/cybercrime/communique.htm*. Los jefes de Estado o de Gobierno hicieron suyo el plan de acción en 1998. Dicho plan ha sido recomendado a otras organizaciones internacionales como la Organización de los Estados Americanos y la Unión Europea.

[8] *Revista Internacional de Política Criminal*, Nos. 43 y 44, 1994 (publicación de las Naciones Unidas, N° de venta S.94.IV.5).

[9] Como la World Justice Information Network <*http://www.justinfo.net*> o el Police Officer Internet Directory <*http://www.officer.com/c_crimes.htm*>.

This archiving project is a collaborative effort between the United Nations Office on Drugs and Crime and the American Society of Criminology, Division of International Criminology. Any comments or questions should be directed to Cindy J. Smith at cjsmithphd@comcast.net or Emil Wandzilak at emil.wandzilak@unodc.org.