Naciones Unidas A/CONF.187/L.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
16 de abril de 2000
Español
Original: inglés

Temas 5 del programa
Prevención eficaz del delito: adaptación a las nuevas situaciones

Informe de la Comisión II

Curso práctico sobre delitos relacionados con las redes informáticas

Introducción

1. El curso práctico sobre delitos relacionados con las redes informáticas, organizado por el Instituto de Asia y el Lejano Oriente para la Prevención del Delito y el Tratamiento del Delincuente, se celebró el 15 de abril de 2000. Se presentó al curso un documento de antecedentes sobre el particular (A/CONF.187/10).

2. El Director del Instituto, Sr. Mikinao Kitada, formuló una declaración introductoria.

3. En un discurso de fondo, la Honorable Sra. Anne Mc Lellan, Ministra de Justicia y Fiscal General del Canadá, señaló la creciente gravedad de la delincuencia informática nacional y transnacional así como la importancia de establecer leyes y procedimientos eficaces para combatirla sin interferencias indeseables en los efectos lícitos y beneficiosos de las nuevas tecnologías.

4. Como parte del curso se celebró una serie de deliberaciones a cargo de grupos de expertos. El primero de ellos examinó la criminología de la delincuencia informática. El segundo grupo analizó, en un marco hipotético de estudios de casos, las cuestiones técnicas y jurídicas derivadas de una búsqueda e incautación legales de datos de redes informáticas. El tercer grupo realizó, en un marco hipotético, un estudio de casos de rastreo de comunicaciones por computadora en redes multinacionales. El cuarto y último grupo deliberó sobre las relaciones existentes entre la aplicación coercitiva de la ley y las ramas de actividad relacionadas con la informática e Internet. En el curso de las deliberaciones hicieron declaraciones los representantes de nueve gobiernos y 17 expertos[*].

[*] La lista de expertos figura en el anexo del presente informe.

Debate general

5. Se señaló que el desarrollo de nuevas tecnologías había proporcionado oportunidades inéditas a los delincuentes. Se había adoptado la expresión “delito relacionado con computadoras” que englobaba tanto las formas completamente nuevas de delincuencia dirigidas a las computadoras, las redes y sus usuarios, como las formas de delito más tradicionales que ahora se cometían con el uso o la ayuda de equipo informático. Se hizo un examen de la respuesta legal a los nuevos delitos. En este aspecto se subrayó que, dada la facilidad con que los mismos podían cometerse más allá de las fronteras nacionales, era importante establecer leyes penales adecuadas en todos los países.

6. Se señaló que el nuevo entorno creado por las redes informáticas ponía a prueba muchos de los supuestos clásicos de los regímenes jurídicos. Se analizó la necesidad de modernizar las leyes para adaptarlas a la tecnología. Se puso de relieve que en las leyes penales se empleaban comúnmente nociones jurídicas tales como las de propiedad, robo y tenencia, pero que esas nociones no eran necesariamente aplicables a los datos informáticos que, por su naturaleza, eran incorpóreos. La facilidad con que los datos podían modificarse había originado también nuevos problemas legales relacionados con su recopilación, conservación y utilización como prueba en procesos.

7. Se hizo observar que las facultades y técnicas necesarias para la investigación eficaz de redes informáticas suscitaban también considerables preocupaciones desde el punto de vista de los derechos humanos y la vida privada, a causa de su naturaleza indiscreta y de los enormes volúmenes de información personal y de otro tipo acumulados y transmitidos por dichas redes. Se convino en que una de las cuestiones fundamentales a que se enfrentaban los gobiernos en el presente y el futuro era la necesidad de llegar a un equilibrio adecuado entre el derecho de cada ciudadano a la vida privada y el interés de la aplicación de la ley. Se señaló que podían surgir cuestiones relativas a la vida privada en buen número de situaciones. También se hizo observar que las leyes de algunos países distinguían entre la búsqueda e interceptación de datos en fase de transmisión y la búsqueda de datos almacenados, mientras que en otras jurisdicciones esa distinción posiblemente no estaba clara. Se señaló que cuando los datos se consideraban comunicaciones en fase de transmisión y, en consecuencia, susceptibles de interceptación en lugar de incautación, pudiera ser necesario aplicar requisitos más rigurosos a la obtención de las autorizaciones necesarias y a las garantías relativas a la forma de realizar la búsqueda. A ese respecto, se consideró que las pruebas buscadas por los órganos de aplicación coercitiva de la ley podrían resultar entremezcladas con otros datos tales como los relativos a negocios o a la situación médica de la persona en cuestión o de un tercero.

8. Se observó que se planteaban muchos problemas cuando las autoridades trataban de obtener información de los proveedores de servicios de Internet. Entre ellos se mencionaron el problema práctico de encontrar a una persona en la sede de un proveedor con la que se pudiera establecer contacto cuando fuera necesario, y el problema jurídico de si el proveedor podía revelar la información voluntariamente o no. Se señaló que las leyes de protección de la esfera privada o de los datos de algunos países prohibían a los proveedores revelar una parte o la totalidad de la información relacionada con las comunicaciones de sus clientes sin una orden judicial, y que las leyes también podían resultar poco claras en cuanto a si los proveedores debían retener los registros sobre los contenidos o las transacciones a fin de que pudieran recuperarse posteriormente si una investigación así lo requería.

9. Varios participantes observaron que cuando las pruebas que buscaban los servicios de aplicación de la ley estaban en los sistemas informáticos de una empresa legítima, la búsqueda podía perjudicar a la empresa si interfería en las operaciones informáticas. Se convino en que, en esos casos, era fundamental ejecutar la búsqueda eficazmente pero sin perturbar el normal desarrollo de las operaciones comerciales.

10. Se consideró que la dimensión transnacional de muchos delitos informáticos podía plantear incluso mayores complicaciones, entre las que cabía destacar las relacionadas con la jurisdicción. Las cuestiones de la legislación de qué país debía aplicarse, las facultades de investigación para obtener pruebas y rastrear o identificar a los delincuentes, la facultad de extraditar a los delincuentes y juzgarlos posteriormente dependían todas en cierta medida del lugar en el que se había cometido el delito; la determinación del lugar resultaría poco clara si el delito se había cometido en más de un sitio mediante el uso de tecnologías de redes informáticas. Se citó el ejemplo de un sitio en la *Web* en un país que contenía especulaciones fraudulentas acerca de una empresa cuyas acciones se negociaban en la bolsa de otro país. Por consiguiente, el delito podía haber ocurrido en uno de los países, o en el otro, o en ambos o en ninguno de ellos, según las leyes de los países involucrados.

11. Se observó que las medidas de búsqueda e incautación también se complicaban cuando los investigadores estaban situados en una jurisdicción y las pruebas se encontraban en otra. Un registro de una red, por ejemplo, podía revelar la existencia de pruebas almacenadas en un país diferente, lo que suscitaba la cuestión de si era necesario el permiso de las autoridades del segundo país para obtener las pruebas, o si se debía notificar a las autoridades del segundo país de que ese registro se estaba realizando. Se observó que cuando era necesario solicitar ayuda por los canales oficiales de la asistencia judicial recíproca, el tiempo requerido para obtener esa asistencia podía ser considerable. La cuestión de cómo podía acelerarse ese proceso podía resultar de fundamental importancia para diligenciar los casos en los que se estaba cometiendo un delito relacionado con computadoras, o cuando las pruebas podían destruirse mientras se tramitaba la asistencia judicial por los canales existentes.

12. Se observó que otra cuestión planteada por la naturaleza transnacional de los delitos relacionados con computadoras y la facilidad con que podían alterarse las pruebas electrónicas era el problema de determinar la autenticidad de las pruebas obtenidas en una búsqueda transfronteriza. Esta determinación podía requerir el establecimiento de procedimientos o protocolos para su uso en búsquedas informáticas a fin de garantizar la autenticidad de los datos recuperados, así como de procedimientos transparentes y seguros que permitieran determinar la autenticidad. Se observó también que en algunos países podían existir requisitos formales que impidieran la utilización de datos electrónicos como prueba.

13. Hubo acuerdo general en que los Estados debían tratar de armonizar, cuando procediera, las disposiciones pertinentes sobre tipificación de delitos, pruebas y procedimientos.

Conclusión

14. El curso práctico llegó a las conclusiones siguientes:

a) Los delitos relacionados con computadoras debían tipificarse;

b) Se requerían leyes procesales adecuadas para la investigación y el enjuiciamiento de los delincuentes cibernéticos;

c) El gobierno y la industria debían aunar esfuerzos en pos del objetivo común de prevenir y combatir los delitos cibernéticos a fin de que Internet se volviera un lugar seguro;

d) Se necesitaba una mayor cooperación internacional para rastrear delincuentes en Internet;

e) Las Naciones Unidas debían adoptar nuevas medidas con respecto al suministro de cooperación y asistencia técnicas en lo que respecta a los delitos relacionados con las redes informáticas.

Anexo I

Expertos participantes en las deliberaciones de expertos

Sr. Shri L.C. Amarnathan, Jefatura de Policía de Sikkim (India)

Sr. Cormac Callanan, Asociación Europea de Proveedores de Servicios de Internet (Irlanda)

Sr. Peter N. Grabosky, Instituto Australiano de Criminología

Sr. Masahito Inoue, Universidad de Tokio (Japón)

Sr. Nigel Jones, Asociación de Jefes de Policía (Reino Unido de Gran Bretaña e Irlanda del Norte)

Sr. Ekkehart Kappler, Oficina Penal Federal (Alemania)

Sr. Henrik W.K. Kaspersen, Profesor de la Universidad Vrije de Amsterdam (Países Bajos)

Sra. Margo L. Langford, Abogada y Procuradora (Canadá)

Sr. Victor Lo, Cuerpo de Policía de Hong Kong (China)

Sr. Keith Mitchell, London Internet Exchange (Reino Unido de Gran Bretaña e Irlanda del Norte)

Sr. Hans G. Nilsson, Consejo de la Unión Europea

Sr. Donald K. Piragoff, Departamento de Justicia (Canadá)

Sra. Mary Riley, Servicio Secreto de los Estados Unidos (Estados Unidos de América)

Sr. Gregory P. Schaffer, Consultor de Seguridad Informática (Estados Unidos de América)

Sr. Ulrich Sieber, Universidad de Munich (Alemania)

Sr. Vittorio Stanca, Dependencia Nacional de Delitos Informáticos (Italia)

Sr. Michael Sussmann, Departamento de Justicia (Estados Unidos de América)