

Distr. limitada
27 de marzo de 2019
Español
Original: inglés

Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético

Viena, 27 a 29 de marzo de 2019

Proyecto de informe

Adición

II. Lista de recomendaciones y conclusiones preliminares (continuación)

A. Aplicación de la ley e investigaciones

1. De conformidad con el plan de trabajo, el presente párrafo contiene una recopilación de las propuestas formuladas por los Estados Miembros en la reunión en relación con el tema 2 del programa, titulado “Aplicación de la ley e investigaciones”. Las recomendaciones y conclusiones preliminares que figuran a continuación fueron presentadas por los Estados Miembros, y su inclusión en este documento no implica que el Grupo de Expertos las haya hecho suyas.

III. Resumen de las deliberaciones

A. Aplicación de la ley e investigaciones (continuación)

2. En el debate subsiguiente, el Grupo de Expertos prestó atención a algunos ejemplos de supuestas actividades delictivas realizadas en el entorno digital y que planteaban importantes dificultades a los profesionales e investigadores de la justicia penal al abrir y llevar a cabo una investigación y, posteriormente, durante el juicio. Entre esos ejemplos figuraban el fraude en línea, el uso de Internet con fines terroristas, el uso de la web oscura para cometer actividades ilícitas, así como el abuso y la explotación sexuales de niños mediante el uso indebido de las tecnologías de la información y las comunicaciones. Además, se informó al Grupo de Expertos sobre la interdependencia conceptual entre la ciberdelincuencia y la ciberseguridad, así como sobre las tendencias y los retos relacionados con la ciberdelincuencia, incluidos los ataques con programas secuestradores (*ransomware*); las tácticas de ingeniería social utilizadas para cometer fraude (*phishing*, *phishing* personalizado, *phishing* de voz, *phishing* de SMS); el uso de la plataforma Cobalt Strike para lanzar ataques contra el sistema bancario; la Internet de las cosas; la extracción y la extracción maliciosa de criptomonedas; y la clonación de tarjetas y delitos conexos.



3. En la reunión del Grupo de Expertos tuvo lugar una vez más el debate sobre si se necesitaba o no un nuevo instrumento jurídico sobre ciberdelincuencia amplio de alcance mundial o si, por el contrario, los Estados deberían centrarse en aplicar de manera efectiva los instrumentos que ya existían, incluido el Convenio sobre la Ciberdelincuencia del Consejo de Europa (Convenio de Budapest). Por una parte, se sostuvo que no se necesitaba un nuevo instrumento jurídico sobre ciberdelincuencia amplio de alcance mundial, dado que el Convenio de Budapest ofrecía un marco adecuado para elaborar respuestas adecuadas de cooperación contra el delito cibernético a nivel nacional e internacional. Se recordó que el hecho de que el Convenio de Budapest tuviera 63 Estados partes demostraba que este estaba abierto a la adhesión de Estados no miembros del Consejo de Europa. Además, se sostuvo que el Convenio era utilizado por terceros Estados partes en él como fuente de inspiración para armonizar las normas legislativas nacionales de carácter sustantivo y procesal. También se expresó que la noción de “armonización de las normas nacionales” incluía no solo casos de convergencia y definiciones comunes, sino también casos en que las normas internacionales eran “útiles” para la elaboración de reglamentaciones nacionales. Se mencionó la complementariedad del Convenio de Budapest con otros instrumentos regionales, como la Convención de la Unión Africana sobre la Confianza y la Seguridad en el Ciberespacio (2014) y el Código Internacional de Conducta para la Seguridad de la Información, publicado por la Organización de Cooperación de Shanghái.

4. Por otra parte, se señaló que era necesario adoptar un nuevo instrumento jurídico sobre ciberdelincuencia de alcance mundial en el marco de las Naciones Unidas para hacer frente a los retos derivados del rápido desarrollo de la tecnología de Internet que no se trataban en los mecanismos existentes, en los que no todos los Estados del mundo eran partes. Se destacó que ese instrumento se elaboraría en el marco de un proceso dirigido por las Naciones Unidas en el que todos los Estados Miembros pudieran asumir como propia la tarea de racionalizar los esfuerzos encaminados a buscar respuestas mundiales al delito cibernético y responsabilizarse de ella, haciendo balance de los instrumentos existentes, como el Convenio de Budapest y la mencionada Convención de la Unión Africana, o tomándolos como base. En ese contexto, se hizo referencia al resolución [73/187](#) de la Asamblea General, de 18 de diciembre de 2018, relativa a los problemas a que se enfrentaban los Estados Miembros en la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, y al mandato que en esta se encomendó al Secretario General de recabar las opiniones de los Estados Miembros sobre los problemas a que se enfrentaban en la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos y de presentar un informe basado en esas opiniones para que la Asamblea General lo examinase en su septuagésimo cuarto período de sesiones. En otras intervenciones se expresó la opinión de que el Convenio de Budapest no abordaba las preocupaciones de todos los Estados Miembros de las Naciones Unidas y que el proceso previsto para modificar el texto del Convenio era muy complejo, lo cual podía ser una desventaja en vista de que la ciberdelincuencia estaba en constante evolución.

5. Se hizo referencia al proceso de negociación que se había puesto en marcha para aprobar un segundo protocolo adicional al Convenio de Budapest destinado a establecer normas claras y procedimientos más eficaces en relación con las siguientes cuestiones: disposiciones para entablar una cooperación internacional más rápida y eficaz; disposiciones que permitieran entablar una cooperación directa con proveedores de servicios de otras jurisdicciones con respecto a las solicitudes de información sobre los abonados, las solicitudes de preservación de datos y las solicitudes de emergencia; un marco más claro y unas salvaguardias más firmes para las prácticas existentes de acceso transfronterizo a los datos; y salvaguardias, incluidos requisitos de protección de datos.

6. También se subrayó que la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional podría ser un instrumento útil para hacer frente a los retos relacionados con la ciberdelincuencia, en particular en vista de su carácter transnacional. Se propuso que se estudiara la posibilidad de negociar un nuevo protocolo de la Convención que se ocupara específicamente del delito cibernético.

7. Las delegaciones y los panelistas informaron al Grupo de Expertos acerca de las iniciativas que se habían puesto en marcha a nivel nacional con resultados satisfactorios para establecer y aplicar medidas jurídicas y de procedimiento destinadas a combatir el delito cibernético. Para algunos, el Convenio de Budapest y los proyectos de creación de capacidad que lo acompañaban eran elementos esenciales en este ámbito. Se examinó a fondo la cuestión de las reformas legislativas a nivel nacional, incluido el alcance de dichas reformas. Se puso de relieve la necesidad de contar con procesos inclusivos y participativos para que se tuvieran en consideración las opiniones de los diferentes interesados. Se hizo referencia a la necesidad de garantizar la seguridad y claridad jurídicas conforme al principio *nullum crimen, nulla poena sine lege*, así como a la necesidad de utilizar un lenguaje “tecnológicamente neutro” en la nueva legislación, de modo que siguiera siendo compatible con los rápidos avances en el ámbito de las tecnologías de la información y las comunicaciones.

8. Las deliberaciones también giraron en torno a los problemas que planteaban los conflictos relacionados con la jurisdicción ejecutiva, especialmente en casos en los que, por ejemplo, un proveedor de servicios tuviera su sede en un país mientras que el responsable del tratamiento de los datos se encontrase en otro o los datos se hallasen almacenados en otro u otros países. Se señaló que la aparición de la computación en la nube planteaba nuevos problemas prácticos y jurídicos para las investigaciones penales. También se señaló que podría resultar útil enfocar de manera flexible la cuestión de las bases jurisdiccionales aplicables en el ámbito de la ciberdelincuencia, por ejemplo concediendo más importancia al lugar desde el que se prestaban los servicios de tecnologías de la información y de las comunicaciones y menos importancia a la ubicación de los datos.

9. El Grupo de Expertos también subrayó la necesidad de disponer de competencias procesales adecuadas para obtener pruebas electrónicas no solo de los delitos cibernéticos, sino también de los delitos convencionales. Esas pruebas electrónicas podían consistir en información sobre los abonados, datos sobre el contenido o datos de tráfico, entre otras cosas. Se señaló que, a medida que aparecían nuevos avances tecnológicos como, por ejemplo, el software de anonimato, el cifrado de alto nivel y las monedas virtuales al investigar delitos en los que entraban en juego pruebas electrónicas, los investigadores tal vez tuvieran que adoptar estrategias nuevas y considerar de qué manera se podrían emplear técnicas de investigación especiales y técnicas forenses digitales remotas para obtener esas pruebas electrónicas y, al mismo tiempo, garantizar su admisibilidad y uso en los tribunales.

10. Durante las deliberaciones también se abordó la manera de lograr un equilibrio entre la necesidad de articular respuestas eficaces a la ciberdelincuencia desde el punto de vista de los organismos encargados de hacer cumplir la ley y la protección de los derechos humanos fundamentales, en especial el derecho a la privacidad. El denominador común fue que, por ejemplo, las normas sobre conservación de datos podrían representar un enfoque pragmático que hiciera posible que los proveedores de servicios de comunicaciones tuvieran más protagonismo en la lucha contra la ciberdelincuencia mediante una mayor cooperación con los organismos encargados de hacer cumplir la ley, siempre y cuando esas normas se aplicasen con las debidas salvaguardias de procedimiento y protección de la privacidad. Se hizo referencia al informe de la Alta Comisionada de las Naciones Unidas para los Derechos Humanos sobre “El derecho a la privacidad en la era digital”, presentado ante el Consejo de Derechos Humanos de conformidad con la resolución [68/167](#) de la Asamblea General ([A/HRC/27/37](#)).

11. El Grupo de Expertos reiteró la importancia de la cooperación internacional en la investigación transfronteriza y el enjuiciamiento de los delitos cibernéticos. Se reconoció que el número de solicitudes de asistencia judicial recíproca para obtener o preservar pruebas electrónicas estaba aumentando rápidamente y que las modalidades de cooperación existentes, especialmente los largos procesos de asistencia judicial recíproca, eran insuficientes para vencer los obstáculos que impedían acceder a los datos con rapidez y eficacia debido al carácter inestable de esas pruebas, que se podían trasladar o borrar “con un simple clic del ratón”.

12. Se mencionaron diferentes ejemplos de prácticas para promover la cooperación internacional en lo que concierne a las pruebas electrónicas, sobre todo a nivel operacional, en particular las siguientes: la transmisión directa de las solicitudes de asistencia judicial recíproca entre las autoridades competentes de los Estados cooperantes; el uso más frecuente de instrumentos de cooperación internacional a la medida para salvaguardar la integridad de las pruebas electrónicas, por ejemplo la conservación rápida de datos informáticos; las investigaciones conjuntas (“equipos mixtos de investigación”); la utilización de medios electrónicos para transmitir las solicitudes de asistencia judicial recíproca, con mención específica de la posible utilidad de la iniciativa de INTERPOL relativa a la transmisión electrónica segura de las comunicaciones sobre la asistencia judicial recíproca (e-MLA); el intercambio de información entre los puntos de contacto de la Red 24/7; y un recurso más frecuente a la cooperación entre fuerzas policiales, entre otras maneras, con la asistencia de INTERPOL, para recabar información de inteligencia. También se hizo referencia al Centro Europeo contra la Delincuencia Informática, establecido por INTERPOL en 2013 para reforzar las respuestas a la ciberdelincuencia de los organismos encargados de hacer cumplir la ley de la Unión Europea.

13. El Grupo de Expertos también trató la cuestión del acceso transfronterizo a los datos. De manera global se señaló que las prácticas y los procedimientos seguidos por los Estados, así como las condiciones y salvaguardas de esos procedimientos, variaban considerablemente. Además se hizo hincapié en los derechos procesales de los sospechosos, las consideraciones relativas a la privacidad y la protección de los datos personales, la legalidad del acceso a los datos almacenados en otro país y el respeto de la soberanía nacional.

14. El Grupo de Expertos recalcó la importancia de la creación sostenible de capacidad para mejorar la eficacia y las cualificaciones de todas las autoridades competentes a nivel operacional a fin de hacer frente a los retos que planteaba la ciberdelincuencia. En ese contexto, los oradores se refirieron a la utilidad de que los profesionales intercambiasen buenas prácticas y experiencias, no solo dentro de cada Estado sino también entre Estados. Algunos oradores se refirieron también a la mejora de la capacitación y la creación de capacidad, sumada al establecimiento de estructuras o unidades especializadas en ciberdelincuencia en el ministerio público y las fuerzas del orden. A ese respecto se destacó que, dado que las pruebas electrónicas también eran cada vez más comunes en las investigaciones de los delitos convencionales, era indispensable crear estructuras especializadas en la investigación de esos delitos que contasen con conocimientos técnicos y competencias operacionales específicos.

15. Asimismo, el Grupo de Expertos deliberó sobre la cooperación de las autoridades nacionales con el sector privado, y especialmente con los proveedores de servicios de comunicaciones, con miras a mejorar la conservación de los datos y el acceso a estos. Aunque se subrayó la importancia cada vez mayor de esa cooperación a escala nacional, especialmente en situaciones de urgencia relacionadas con delitos graves, también se reconoció la necesidad de intensificar los esfuerzos para alcanzar un grado similar de cooperación en los casos transnacionales. A ese respecto se mencionó el denominado “riesgo del cumplimiento doble” para los mencionados proveedores, es decir, la dificultad de equilibrar sus respuestas conforme a los requisitos legales de los Estados implicados.

IV. Organización de la reunión

B. Declaraciones (*continuación*)

16. Formularon declaraciones los expertos de los siguientes Estados: Argelia, Burkina Faso, Canadá, Chile, China, Colombia, Francia, India, Italia, Japón, Kuwait, Mauritania, Países Bajos, Noruega y Sri Lanka.

17. También formuló una declaración la Unión Europea, organización intergubernamental.
