Distr. limitada
28 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

A. Aplicación de la ley e investigaciones (*continuación*)

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 supone que el Grupo de Expertos las haya hecho suyas; el orden en que se presentan tampoco implica una valoración de su importancia:

a) Por una parte, se propuso que los Estados Miembros articularan nuevas respuestas internacionales contra el delito cibernético tomando en consideración la posibilidad de negociar un nuevo instrumento jurídico contra la ciberdelincuencia de alcance mundial en el marco de las Naciones Unidas que tuviera en cuenta las inquietudes y los intereses de los Estados Miembros, teniendo en cuenta también, entre otras cosas, el proyecto de convención de las Naciones Unidas sobre cooperación en la lucha contra la ciberdelincuencia presentado al Secretario General el 11 de octubre de 2017 (A/C.3/72/12, anexo);

b) Por otra parte, se propuso que no era ni necesario ni apropiado considerar la posibilidad de un nuevo tratado de alcance mundial porque el mejor modo de afrontar los retos del delito cibernético y la debida capacitación de los investigadores, fiscales y jueces era la creación de capacidad, el diálogo activo y la cooperación entre los organismos encargados de hacer cumplir la ley y la utilización de las herramientas disponibles, como el Convenio de Budapest. De acuerdo con esta propuesta, los Estados Miembros deberían seguir adoptando y utilizando los instrumentos jurídicos multilaterales sobre ciberdelincuencia en vigor, como el Convenio de Budapest, que muchos Estados consideraban el instrumento de orientación más apropiado y específico, tanto de carácter sustantivo como de procedimiento, para elaborar una legislación nacional apropiada en materia de ciberdelincuencia a fin de facilitar la cooperación internacional para combatir esos delitos;

c) Habida cuenta del carácter transnacional de la ciberdelincuencia y del hecho de que la gran mayoría de los delitos cibernéticos a nivel mundial son cometidos por grupos organizados, los Estados Miembros también deberían hacer mayor uso de la

Convención contra la Delincuencia Organizada para facilitar el intercambio de información y pruebas para la investigación penal de esos delitos;

d) Los Estados miembros deberían promover y entablar iniciativas de cooperación internacional contra la ciberdelincuencia, haciendo uso de los instrumentos existentes y celebrando acuerdos bilaterales basados en el principio de reciprocidad, así como apoyando, en colaboración con la UNODC, el establecimiento de redes de contactos y el intercambio de información entre las autoridades judiciales y las fuerzas del orden de forma periódica;

e) Los países deberían desarrollar los conocimientos especializados en investigación de delitos cibernéticos de los organismos policiales mediante su participación en las actividades de capacitación que imparten numerosos países, así como la UNODC y otros asociados regionales, que tienen por objeto desarrollar la capacidad de detección e investigación de la ciberdelincuencia y fortalecer la capacidad colectiva para combatir ese tipo de delitos. Las actividades de creación de capacidad en esta esfera deberían atender, en particular, las necesidades de los países en desarrollo, centrarse en las vulnerabilidades de cada país a fin de garantizar una asistencia técnica adaptada a sus necesidades y promover el intercambio de los conocimientos más avanzados en interés de los beneficiarios;

f) Se alienta a los Estados a que sigan dotando a la UNODC de los mandatos y el apoyo financiero necesarios con miras a obtener resultados tangibles en los proyectos de creación de capacidad en esta esfera;

g) Los países deberían destinar recursos a generar los conocimientos especializados necesarios para investigar la ciberdelincuencia y establecer alianzas para utilizar los mecanismos de cooperación con miras a obtener pruebas críticas;

h) Los Estados Miembros deberían seguir esforzándose por crear y apoyar dependencias, órganos o estructuras especializados en ciberdelincuencia en las fuerzas del orden, el ministerio público y la judicatura, dotándolos de los conocimientos especializados y el equipo necesarios para hacer frente a los retos que plantean esos delitos y para reunir, compartir y utilizar pruebas electrónicas en los procedimientos penales;

i) Teniendo presente que la lucha contra la ciberdelincuencia exige estrategias de aplicación de la ley a mediano y largo plazo que incluyan iniciativas de cooperación con los asociados internacionales para desmantelar los mercados de la ciberdelincuencia, esas estrategias deberían ser proactivas y estar dirigidas, preferiblemente, contra los grupos delictivos organizados implicados en ese tipo de actividades, cuyos integrantes se encuentran en numerosos países;

j) Los países deberían seguir esforzándose por promulgar leyes de carácter sustantivo que traten las formas nuevas y emergentes de delincuencia en el ciberespacio en un lenguaje neutral desde el punto de vista tecnológico para garantizar su compatibilidad con los futuros avances en la esfera de las tecnologías de la información y de las comunicaciones;

k) El derecho procesal interno debe ser capaz de seguir el ritmo de los avances tecnológicos para que los organismos encargados de hacer cumplir la ley dispongan de medios adecuados para combatir la delincuencia en línea. Deberían redactarse leyes pertinentes teniendo presentes los conceptos técnicos aplicables, así como las necesidades prácticas de los investigadores de delitos cibernéticos, de conformidad con las normas del debido proceso, los intereses de privacidad, las libertades civiles y los derechos humanos, así como los principios de proporcionalidad y subsidiariedad y las salvaguardias que garantizan la supervisión judicial. Además, los Estados Miembros deberían dedicar recursos a promulgar leyes nacionales para autorizar lo siguiente:

i) solicitudes de conservación rápida de datos informáticos a la persona que tiene el control de estos, es decir, los proveedores de servicios de Internet y comunicaciones, con objeto de proteger y mantener la integridad de los datos durante un período determinado debido a la posible inestabilidad de esos datos;

ii) registro e incautación de datos de contenido almacenados en dispositivos digitales, que suelen ser las pruebas de la comisión de un delito electrónico más importantes para demostrar su atribución;

iii) órdenes para obtener datos informáticos que tengan menor nivel de protección de la privacidad, como los datos de tráfico y los datos de los abonados;

iv) obtención en tiempo real de datos de tráfico y contenido en los casos en que proceda; y

v) autorización para que los organismos nacionales encargados de hacer cumplir la ley puedan entablar relaciones de cooperación internacional.

l) Dado que las investigaciones de delitos cibernéticos requieren creatividad, ingenio técnico y esfuerzos conjuntos entre el fiscal y la policía, los países deberían alentar una estrecha colaboración entre el ministerio público y las fuerzas policiales en las primeras etapas de la investigación a fin de obtener pruebas suficientes para proceder penalmente contra las personas identificadas;

m) Los funcionarios encargados de hacer cumplir la ley deberían contar con el asesoramiento de investigadores al investigar casos de ciberdelincuencia para garantizar que se respeten las normas del debido proceso;

n) Los organismos nacionales encargados de hacer cumplir la ley deberían ponerse en contacto y colaborar con los proveedores nacionales de servicios de Internet y otros grupos del sector privado. Este contacto sirve de apoyo a las investigaciones de los organismos encargados de hacer cumplir la ley, ya que fortalece la confianza y la cooperación entre las partes interesadas;

o) Los países podrían 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 prestan los servicios de tecnologías de la información y de las comunicaciones y menos importancia a la ubicación de los datos.

p) Los países deberían invertir en la educación de la comunidad y del sector para crear mayor conciencia sobre la ciberdelincuencia a fin de aumentar la tasa de denuncia de los delitos cibernéticos, que es inferior a la de otro tipo de delitos;

q) Los Estados Miembros deberían fomentar las alianzas público-privadas en la esfera de la ciberdelincuencia, entre otras cosas mediante la promulgación de legislación y el establecimiento de vías de diálogo a tal efecto, a fin de promover la cooperación entre las autoridades encargadas de hacer cumplir la ley y los proveedores de servicios de comunicaciones, así como con las instituciones académicas, con miras a aumentar los conocimientos y a mejorar la eficacia de las respuestas al delito cibernético.

III. Resumen de las deliberaciones

A. Aplicación de la ley e investigaciones *(continuación)*

2. Muchos oradores informaron acerca de medidas nacionales encaminadas a elaborar y aplicar estrategias y políticas de ciberseguridad; promulgar legislación sobre ciberdelincuencia o mejorar la ya existente; utilizar nuevos instrumentos de investigación para obtener pruebas electrónicas y determinar su autenticidad a efectos probatorios en procedimientos penales, teniendo en cuenta las salvaguardias de los derechos humanos; poner en práctica acuerdos institucionales para hacer un uso más eficiente de los recursos contra la ciberdelincuencia; y promover la cooperación internacional contra la ciberdelincuencia. Un orador se refirió a las diferencias entre la ciberseguridad y la ciberdelincuencia, y señaló que era importante tener en cuenta esa distinción al estructurar las respuestas nacionales y definir las competencias institucionales en la materia.

3. Numerosos oradores apoyaron la labor del Grupo de Expertos, al que consideraron el único foro amplio, y el más adecuado, a nivel mundial para facilitar el debate y el intercambio de opiniones entre los Estados Miembros en relación con la legislación nacional, las mejores prácticas, la asistencia técnica y la cooperación internacional, con miras a examinar opciones para fortalecer las respuestas jurídicas o de otra índole al delito cibernético en los planos nacional e internacional. En ese sentido, también se mencionó el valor añadido de la Comisión de Prevención del Delito y Justicia Penal. Se sugirió que, si bien el Grupo de Expertos tenía el mandato único de actuar como plataforma para los debates en ese ámbito, ello no excluía necesariamente otras iniciativas destinadas a desarrollar una "gobernanza global", de carácter amplio, contra la ciberdelincuencia a nivel internacional.

4. Se hizo referencia a un acto paralelo celebrado durante la reunión del Grupo de Expertos, que había llevado por título "Enfoques para hacer frente a la ciberdelincuencia: perspectivas desde ambos lados del Pacífico y más allá". El acto paralelo había estado organizado por los Gobiernos de Australia, los Estados Unidos, la República Dominicana, Samoa y Vanuatu.

5. Se expresó apoyo a la UNODC por su labor en la esfera de la asistencia técnica y la creación de capacidad para dar respuestas bien cohesionadas a la ciberdelincuencia.

6. Algunos oradores también expresaron su reconocimiento por la publicación de la guía práctica para la solicitud de pruebas electrónicas transfronterizas (*Practical Guide for Requesting Electronic Evidence Across Borders*). La guía había sido redactada y presentada conjuntamente por la UNODC, la Dirección Ejecutiva del Comité contra el Terrorismo (DECT) y la Asociación Internacional de Fiscales, y se había puesto a disposición de los Estados Miembros y sus funcionarios de justicia penal en el portal SHERLOC de la UNODC. Se había elaborado en colaboración con los Estados Miembros, otras organizaciones internacionales y regionales, y proveedores de servicios de comunicaciones como Facebook, Google, Microsoft y Uber, y contenía información para ayudar a determinar medidas nacionales destinadas a reunir, preservar y compartir pruebas electrónicas con el objetivo general de asegurar la eficiencia en la práctica de la asistencia judicial recíproca.

IV. Organización de la reunión

B. Declaraciones *(continuación)*

7. Formularon declaraciones expertos de los siguientes Estados: Armenia, Costa Rica, Emiratos Árabes Unidos, Eslovaquia, España, Estonia, Filipinas, Georgia, Malasia, Marruecos, México, Paraguay, Perú, República Dominicana y Tailandia.

8. El Consejo de Europa, organización intergubernamental, también formuló una declaración.