27 de julio de 2020
Español
Original: inglés

Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético
Viena, 27 a 29 de julio de 2020

Proyecto de informe

Adición

II. Lista de recomendaciones y conclusiones preliminares (*continuación*)

A. Cooperación internacional

1. En consonancia con el plan de trabajo del Grupo de Expertos, el presente párrafo contiene una recopilación de las sugerencias formuladas por los Estados Miembros en la reunión en relación con el tema 2 del programa, titulado “Cooperación internacional”. 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; tampoco están presentadas en orden de importancia:

1) En cuanto al alcance de la definición de “delito cibernético” a efectos de cooperación internacional, los países deberían tipificar como delito los actos de ciberdelincuencia en grado suficiente, de modo que quedaran comprendidos no solo los delitos basados en la cibernética, sino también otros delitos cometidos con frecuencia utilizando Internet y medios electrónicos (delitos facilitados por la cibernética), como fraude cibernético, robo cibernético, extorsión, blanqueo de dinero, tráfico de drogas y armas, pornografía infantil y actividades terroristas.

2) En relación con los mecanismos de cooperación internacional, a falta de un tratado bilateral de asistencia judicial recíproca, se alienta a los Estados a que utilicen o se adhieran a los tratados multilaterales existentes que proporcionan una base jurídica para la prestación de asistencia judicial recíproca como el Convenio de Budapest sobre la Ciberdelincuencia y la Convención contra la Delincuencia Organizada; a falta de tratados, los Estados podrían solicitar cooperación sobre la base del principio de reciprocidad; también debería usarse el Convenio de Budapest sobre la Ciberdelincuencia como referencia en la creación de capacidad y la asistencia técnica en todo el mundo, mientras que la atención se dirige en estos momentos a las negociaciones en curso sobre el segundo protocolo adicional del Convenio de Budapest sobre la Ciberdelincuencia para reforzar aún más la cooperación transfronteriza. En otra intervención, se reiteró la opinión de que el Convenio de Budapest sobre la Ciberdelincuencia tenía un ámbito de aplicación limitado por su condición de instrumento regional y su situación en cuanto a las ratificaciones, así como por carecer de un enfoque integral al no tener en cuenta las tendencias actuales en el delito cibernético y no ser plenamente adecuado para los países

V.20-04092 (S) 290720 290720

en desarrollo. Se señaló la atención sobre la resolución 74/247 de la Asamblea General, de 27 de diciembre de 2019, en la que esta decidió establecer un comité intergubernamental especial de expertos de composición abierta, representativo de todas las regiones, a fin de elaborar una convención internacional integral sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos. En cambio, en otras intervenciones se defendió que los nuevos marcos o instrumentos en materia de ciberdelincuencia no deberían ir en contra de los que ya existían ni deberían obligar a los Estados a abandonar o contravenir los tratados vigentes, los compromisos previamente adquiridos o los acuerdos alcanzados.

3) Es necesario contar con socios estratégicos en la investigación del delito cibernético, como los miembros de organizaciones existentes, tales como la Organización de los Estados Americanos, el G7 o INTERPOL.

4) En las investigaciones y los procedimientos judiciales, deben respetarse la soberanía y la jurisdicción de los Estados. No debería solicitarse a empresas o particulares la entrega directa de datos ubicados en otro país sin el consentimiento previo de este.

5) Debería mejorarse la eficiencia de la cooperación internacional estableciendo mecanismos de respuesta rápida para la cooperación internacional, así como canales de comunicación entre las autoridades nacionales mediante oficiales de enlace y sistemas informáticos para la reunión trasfronteriza de pruebas y la transferencia en línea de pruebas electrónicas.

6) Los Estados deberían seguir estrechando la cooperación para proteger las infraestructuras esenciales y fortalecer las redes de colaboración entre los equipos informáticos de respuesta de emergencia (CERT y CSIRT).

7) Los Estados deberían estudiar la posibilidad de crear protocolos innovadores de intercambio de información, incluidas la información de inteligencia y las pruebas de actos delictivos, a fin de agilizar esos procedimientos.

8) Es necesario reafirmar el compromiso de todos los Estados Miembros de garantizar la seguridad de las tecnologías de la información y las comunicaciones utilizándolas exclusivamente con fines pacíficos e intensificando las iniciativas internacionales para combatir las actividades malintencionadas en el ciberespacio en una época de crisis mundial, regional y local profunda.

9) Deberían optimizarse los procedimientos de cooperación internacional para que se preste la máxima asistencia dentro de las posibilidades que ofrezca el marco jurídico nacional a las solicitudes de cooperación internacional relativas a la conservación de pruebas electrónicas, el acceso a la información de conexión y la información de registro de los usuarios que no vulnere los derechos humanos, las libertades fundamentales o los derechos de propiedad.

10) Se exhorta a los países a que presten especial atención a la necesaria proporcionalidad de las medidas de investigación, de modo que se respeten las libertades fundamentales y los regímenes de protección de datos personales asociados con la correspondencia privada.

11) La cooperación internacional en la lucha contra la ciberdelincuencia también debería tener en cuenta enfoques sensibles al género y la edad, así como las necesidades de los grupos vulnerables.

12) En cuanto al alcance de la cooperación internacional, si bien solo deberían prestar asistencia judicial recíproca las autoridades nacionales, la cooperación no debería circunscribirse a los departamentos gubernamentales, sino que también debería implicar al sector privado, por ejemplo a los proveedores de servicios de Internet. En este sentido, se recomendó la aprobación de disposiciones que permitieran entablar una cooperación directa con los proveedores de servicios de Internet de otras jurisdicciones con respecto a las solicitudes de información sobre los abonados, las solicitudes de conservación de datos y las solicitudes de emergencia.

13) Las opciones para combatir la ciberdelincuencia y proteger las sociedades deben salvaguardar siempre los derechos humanos y las garantías constitucionales y promover un ciberespacio más libre, abierto, seguro y resiliente para todas las personas.

14) Se alienta a los países a que simplifiquen la cooperación con el sector privado y a que refuercen la colaboración entre los gobiernos y los proveedores de servicios privados, en particular para hacer frente a los retos que plantea la presencia de material delictivo nocivo en Internet.

15) Las empresas privadas, fundamentalmente los proveedores de servicios de Internet, tienen una responsabilidad compartida en la prevención e investigación del delito cibernético y deberían agilizar y ampliar sus respuestas a las solicitudes de asistencia judicial, ofrecerlas en los países en que estén establecidas y asegurarse de disponer de los canales apropiados para comunicarse con las autoridades locales.

16) Deben reforzarse las alianzas entre los sectores público y privado; en los casos en que no existan esas alianzas, deben crearse, y las empresas privadas deberían participar en grupos de trabajo (foros multilaterales) y en el diálogo abierto para mejorar el enfoque que se sigue frente a los delitos cibernéticos.

17) Las organizaciones no gubernamentales y el mundo académico también deben implicarse en la labor de prevención y lucha contra la ciberdelincuencia, por cuanto aportan una perspectiva inclusiva, plural y amplia con la finalidad, entre otras, de garantizar la protección de los derechos humanos, especialmente la libertad de expresión y el derecho a la vida privada.

18) Se exhorta a los países a que se incorporen, utilicen en mayor medida y refuercen las redes autorizadas de profesionales para conservar e intercambiar pruebas electrónicas admisibles, como las redes operativas de manera ininterrumpida, las redes especializadas en ciberdelincuencia y los canales de INTERPOL para la cooperación interpolicial ágil, así como a que establezcan redes con socios que tengan la misma estrategia, con vistas a intercambiar datos sobre asuntos de ciberdelincuencia, habilitar respuestas rápidas y minimizar la pérdida de pruebas esenciales. En otras intervenciones también se recomendó el uso de la cooperación interpolicial y otros métodos de cooperación oficiosa antes de acudir a los canales de asistencia judicial recíproca.

19) Cada Estado debería establecer un verdadero punto de contacto para las redes operativas de manera ininterrumpida, dotado de los recursos necesarios, para facilitar la conservación de los datos digitales junto con la tradicional asistencia recíproca internacional en asuntos penales, tomando como punto de partida el modelo de éxito de la congelación de datos con arreglo al Convenio del Consejo de Europa.

20) Los países deberían fortalecer la colaboración interinstitucional y deberían mejorar la interoperabilidad estandarizando las solicitudes de información y los procedimientos de autenticación y logrando la aceptación por parte de múltiples interesados.

21) Los países deberían mejorar la aplicación de las leyes nacionales y reforzar la coordinación y la sinergia a nivel interno para la reunión y el intercambio de información y pruebas con fines de enjuiciamiento.

22) Los Estados deberían fortalecer las medidas en lo que respecta al intercambio de información financiera o monetaria, la congelación de cuentas y el decomiso de bienes para garantizar que los delincuentes no puedan beneficiarse de las actividades delictivas.

23) Se alienta a los Estados a que establezcan equipos conjuntos de investigación con otros países en los planos bilateral, regional o internacional para aumentar la capacidad de hacer cumplir la ley.

24) Los Estados también deberían facilitar un tratamiento eficaz de las pruebas electrónicas y la admisibilidad de dichas pruebas ante los tribunales, incluso cuando se destinen a una jurisdicción extranjera o se reciban de ella. A ese respecto, se los alienta a que continúen o inicien reformas de la legislación sobre el delito cibernético y las

pruebas electrónicas, siguiendo los ejemplos positivos y las reformas emprendidas en todo el mundo.

25) Se recomienda elaborar marcos jurídicos que abarquen también los aspectos relacionados con la jurisdicción extraterritorial respecto de los actos de ciberdelincuencia.

26) Los países deberían perfeccionar los mecanismos para mitigar los conflictos y hacer frente a las dificultades relacionadas con la atribución y la capacidad para investigar los casos de ciberdelincuencia.

27) Los Estados deberían tratar de estandarizar y difundir instrumentos procesales para la aportación acelerada de datos y la ampliación de las búsquedas (como las órdenes de entrega de documentos, así como las órdenes de medidas aceleradas de conservación o de acceso transfronterizo, etc.) a fin de facilitar la labor de las autoridades encargadas de hacer cumplir la ley y su cooperación directa con los proveedores de servicios de Internet y resolver los problemas relacionados con el rastreo de las pruebas electrónicas y su utilización adecuada.

28) Los Estados deberían facilitar la elaboración y estandarización de normas técnicas interoperables para la labor forense digital y la recuperación de pruebas electrónicas transfronterizas.

29) Se recomienda invertir en una autoridad central sólida para la cooperación internacional en asuntos penales a fin de garantizar que los mecanismos de cooperación en lo que respecta al delito cibernético también sean eficaces; se recomienda establecer unidades específicas para investigar los delitos cibernéticos; y se recomienda también atender las solicitudes de conservación de otros Estados mediante una red que funcione las 24 horas del día, los 7 días de la semana (o directamente con el proveedor en algunas circunstancias) para preservar los datos necesarios lo más rápidamente posible. Una mayor comprensión de la información que se necesita para que una solicitud de asistencia judicial recíproca sea admitida puede contribuir a que se obtengan los datos más rápidamente.

30) Para que la cooperación internacional sea eficaz, es necesario que las leyes nacionales establezcan procedimientos que permitan la cooperación internacional. Por tanto, la legislación nacional debe posibilitar la cooperación internacional entre los organismos encargados de hacer cumplir la ley.

31) Más allá de las leyes nacionales, la cooperación internacional en materia de ciberdelincuencia se basa tanto en la cooperación oficial fundamentada en tratados como en la asistencia interpolicial tradicional. Al debatir sobre un nuevo instrumento relacionado con el delito cibernético, es importante que los países recuerden que los nuevos instrumentos no deben entrar en conflicto con los instrumentos existentes, que ya hacen posible la cooperación internacional en tiempo real para tantos de ellos. Así pues, los países deben procurar evitar todo conflicto entre los nuevos instrumentos contra el delito cibernético y los tratados existentes.

32) Se debería priorizar y reforzar la creación de capacidad sostenible y la asistencia técnica para aumentar la capacidad en todas las esferas operacionales y fortalecer la capacidad de las autoridades nacionales para responder a la ciberdelincuencia, lo que incluye el establecimiento de redes, la celebración de reuniones y cursos de capacitación conjuntos, el intercambio de mejores prácticas, la facilitación de material de capacitación y la elaboración de plantillas para la cooperación. La creación de capacidad y la capacitación mencionadas deberían incluir una formación altamente especializada para los profesionales que promueva, en particular, la participación de mujeres expertas, y prestar más atención a las necesidades de los siguientes actores: las necesidades de los legisladores y los encargados de formular políticas para tratar mejor las cuestiones relativas a la conservación de datos a efectos de hacer cumplir la ley; las necesidades de las autoridades encargadas de hacer cumplir la ley, los investigadores y los analistas para mejorar su capacidad en la ciencia forense y la utilización de datos de código abierto para las investigaciones, en la cadena de custodia de las pruebas electrónicas y en la reunión y el intercambio de pruebas electrónicas en el extranjero, y las necesidades de

jueces, fiscales, autoridades centrales y abogados para juzgar y tratar eficazmente los casos pertinentes.

33) Es esencial elaborar normas y plazos adecuados, y de ser posible uniformes, de retención y conservación de datos a fin de garantizar que puedan preservarse u obtenerse las pruebas electrónicas para respaldar nuevas solicitudes de asistencia judicial recíproca.

34) El Grupo de los 77 y China reconoce que la cooperación internacional es importante para reunir e intercambiar pruebas electrónicas en el contexto de las investigaciones transfronterizas y que es necesario responder rápida y eficazmente a las solicitudes de asistencia judicial recíproca relativas a la conservación y la obtención de pruebas electrónicas. El Grupo también subraya que durante el proceso deben respetarse los principios de soberanía y reciprocidad.

35) El Grupo de los 77 y China alienta asimismo a la UNODC a que siga ofreciendo programas de creación de capacidad y formación en la lucha contra la ciberdelincuencia a los expertos gubernamentales nacionales, a fin de fortalecer la capacidad de detectar e investigar los delitos cibernéticos. Las actividades de creación de capacidad en esa esfera deberían tener en cuenta las necesidades de los países en desarrollo, centrarse en las vulnerabilidades de cada país a fin de prestar una asistencia técnica adaptada a sus circunstancias y promover el intercambio de los conocimientos más actualizados en interés de los profesionales e interesados.

36) La UNODC ha elaborado el Programa para Redactar Solicitudes de Asistencia Judicial Recíproca a fin de ayudar a los profesionales de la justicia penal a redactar dichas solicitudes. La UNODC también ha elaborado la publicación *Practical Guide for Requesting Electronic Evidence Across Borders* (Guía Práctica para la Solicitud de Pruebas Electrónicas Transfronterizas), que está a disposición de los profesionales de los organismos de los Estados Miembros que la soliciten. Así pues, los países pueden beneficiarse de la utilización de estos instrumentos clave desarrollados por la UNODC.

37) La Comisión de Prevención del Delito y Justicia Penal debería considerar la posibilidad de prorrogar el plan de trabajo del Grupo Intergubernamental de Expertos más allá de 2021 como foro para que los profesionales intercambien información sobre el delito cibernético.

38) Algunos oradores observaron que la negociación y aprobación de una convención de las Naciones Unidas para promover la cooperación en la lucha contra el delito cibernético facilitaría que la cooperación internacional en la lucha contra la ciberdelincuencia fuera más eficiente.

39) Se recomendó que fueran los expertos de la UNODC en Viena quienes se ocuparan de elaborar tal convención.

IV. Organización de la reunión (*continuación*)

C. Declaraciones

2. Formularon declaraciones los expertos de los siguientes Estados Miembros y el siguiente Estado observador no miembro: Argelia, Argentina, Armenia, Brasil, Canadá, Chile, Colombia, Ecuador, Egipto, Estado de Palestina, Estado de Palestina (en nombre del Grupo de los 77 y China), Estados Unidos de América, Federación de Rusia, India, Líbano, México, Noruega, Países Bajos, Portugal y Rumania.