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 algunas intervenciones se recomendó que la Comisión de Prevención del Delito y Justicia Penal renovara el mandato de este grupo intergubernamental de expertos sobre el delito cibernético y adoptara una decisión respecto de un plan de trabajo para después de 2021, que también debería incluir las formas emergentes de delitos cibernéticos y el examen de las cuestiones relacionadas con el abuso sexual de niños y la explotación infantil en Internet.

2. Además, se recomendó que el comité intergubernamental especial de expertos de composición abierta establecido en virtud de la resolución 74/247 de la Asamblea General 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 no iniciara su labor sino hasta después de que el grupo intergubernamental de expertos hubiera finalizado sus recomendaciones y las hubiese enviado a la Comisión de Prevención del Delito y Justicia Penal en 2021.

3. Sin embargo, en otra intervención se afirmó que no era necesario que la labor del grupo intergubernamental de expertos continuara después de 2021, habida cuenta de la aprobación de la resolución 74/247 de la Asamblea General. Esto permitirá centrarse en la aplicación de esa resolución y en la negociación de una nueva convención, así como aprovechar de la mejor manera los recursos financieros disponibles.

4. En sus intervenciones, algunos Estados Miembros acogieron con beneplácito la aprobación de la resolución 74/247 de la Asamblea General. Se afirmó que la elaboración de la nueva convención, de conformidad con la resolución 74/247 de la Asamblea General, debía ser inclusiva, transparente y basarse en el consenso, y que los anteriores procesos de las Naciones Unidas para concertar la Convención contra la Delincuencia Organizada Transnacional y la Convención contra la Corrupción podían constituir un ejemplo destacado en este sentido.

5. Se pidió la participación activa de todos los Estados Miembros en el establecimiento de la labor del comité especial para elaborar una nueva convención.

V.20-04117 (S) 290720 290720

6. Al mismo tiempo, en otras intervenciones se afirmó también que, en lo que respecta al contenido, una nueva convención debería tener en cuenta los marcos e instrumentos existentes y no entrar en conflicto con ellos. Se recomendó que las cuestiones de la obtención transfronteriza de pruebas, las disposiciones en materia de penalización y el respeto de la soberanía se incluyeran en la posible nueva convención.

7. La comunidad internacional debería dar prioridad a la prestación de apoyo para la creación de capacidad y de otro tipo a fin de fortalecer la capacidad de las autoridades nacionales para responder al delito cibernético y, en particular, al abuso sexual de niños y la explotación infantil en Internet.

8. Los Estados Miembros deben prestarse asistencia judicial recíproca para obtener pruebas electrónicas en la mayor medida posible, incluso en casos relacionados con el uso de las tecnologías de la información y las comunicaciones para cometer actos de terrorismo, incitar a su comisión o financiarlos; se afirmó además que las entidades del sector privado tenían la responsabilidad de cooperar con las autoridades nacionales a este respecto.

9. Los Estados Miembros deberían considerar la posibilidad de invertir en fuerzas centralizadas especializadas en el delito cibernético, así como en dependencias tecnológicas regionales de investigación penal.

10. Los Estados Miembros también deberían considerar la posibilidad de establecer dependencias separadas para el delito cibernético dentro de las autoridades centrales para la asistencia judicial recíproca como base de conocimientos especializados en esta compleja esfera de la cooperación internacional. Esas dependencias especializadas no solo aportan beneficios en la práctica cotidiana de la asistencia judicial recíproca, sino que también permiten prestar asistencia específica para el fomento de la capacidad, como la formación para atender a las necesidades de las autoridades nacionales y extranjeras sobre la forma de obtener de manera rápida y eficiente asistencia judicial recíproca que entrañe pruebas electrónicas, en cuestiones relacionadas con los delitos cibernéticos.

11. Los Estados Miembros deberían considerar la posibilidad de mantener bases de datos electrónicas que faciliten el acceso a estadísticas relativas a las solicitudes entrantes y salientes de asistencia judicial recíproca que entrañen pruebas electrónicas, a fin de garantizar que se realicen exámenes de la eficiencia y la eficacia.

12. Se debería recordar a los Estados Miembros que aprovechen el papel fundamental de las autoridades centrales en la transmisión de las solicitudes de asistencia judicial recíproca y en la colaboración con las autoridades competentes para la ejecución de dichas solicitudes a fin de garantizar el cumplimiento de los tratados existentes y reducir las demoras en el proceso.

13. Para obtener datos que permitan realizar investigaciones de actos de ciberdelincuencia, los Estados deberían aprovechar los instrumentos internacionales de probada eficacia, y este complejo tema requiere un marco institucional que haya demostrado su resistencia y valor añadido. A este respecto se puso de relieve el Convenio sobre la Ciberdelincuencia, que ha sido una norma en la obtención de pruebas electrónicas a lo largo de los años y que ha dado resultados concretos a diario para los organismos encargados de hacer cumplir la ley de todo el mundo. Asimismo, se recomendó que los Estados redujeran los conflictos de leyes en relación con los requisitos jurídicos aplicables, teniendo en cuenta, como puntos de partida, en caso de órdenes directas de presentación de datos, la legislación del Estado en que se encuentra el proveedor de servicios de Internet al que se solicita información o la del Estado del sospechoso.

14. Se recomienda crear un marco en el que quede claro que en caso de “pérdida de la ubicación” la decisión de proceder con la investigación requiere un esfuerzo para establecer qué territorio ha sido afectado y donde es vital la integridad de las redes automatizadas para poder realizar consultas sobre cuestiones de jurisdicción y la forma más adecuada de continuar las indagaciones.

15. Se recomendó que fuera aplicable en el ciberespacio el derecho internacional, incluidos los principios de soberanía, integridad territorial y no intervención en los asuntos internos, que no se emplearan las tecnologías de la información y las comunicaciones como armas y que se condenaran los ataques patrocinados por los Estados y se exigieran cuentas a los responsables.

IV. Organización de la reunión (*continuación*)

C. Declaraciones

16. Formularon declaraciones los expertos de los siguientes Estados Miembros: Alemania, Australia, Austria, Azerbaiyán, China, Cuba, España, Filipinas, Francia, Grecia, Honduras, Hungría, Indonesia, Irán (República Islámica del), Iraq, Israel, Italia, Japón, Mongolia, Nigeria, Nueva Zelandia, Paraguay, Polonia, Reino Unido, Tailandia y Venezuela (República Bolivariana de).

17. Formularon declaraciones también los representantes de las siguientes organizaciones intergubernamentales: Consejo de Europa, Organización Internacional de Policía Criminal y Unión Europea. Además, hizo una declaración un observador, la Universidad Normal de Beijing.