Naciones Unidas E/CN.15/2018/12

Consejo Económico y Social

Distr. general
13 de abril de 2018
Español
Original: inglés

Comisión de Prevención del Delito y Justicia Penal
27º período de sesiones
Viena, 14 a 18 de mayo de 2018
Tema 8 del programa provisional*
Tendencias de la delincuencia a nivel mundial y nuevas cuestiones y respuestas relativas a la prevención del delito y la justicia penal

Informe de la reunión del Grupo de Expertos encargado de realizar un Estudio Exhaustivo sobre el Delito Cibernético celebrada en Viena del 3 al 5 de abril de 2018

I. Introducción

1. En su resolución 65/230, la Asamblea General solicitó a la Comisión de Prevención del Delito y Justicia Penal que, con arreglo a lo dispuesto en el párrafo 42 de la Declaración de Salvador sobre Estrategias Amplias ante Problemas Globales: los Sistemas de Prevención del Delito y Justicia Penal y su Desarrollo en un Mundo en Evolución, estableciera un grupo intergubernamental de expertos de composición abierta, que se reuniría con antelación al 20º período de sesiones de la Comisión, para que realizara un estudio exhaustivo del problema del delito cibernético y las respuestas de los Estados Miembros, la comunidad internacional y el sector privado ante ese fenómeno, incluido el intercambio de información sobre legislación nacional, mejores prácticas, asistencia técnica y cooperación internacional, con miras a examinar opciones para fortalecer las actuales respuestas jurídicas o de otra índole ante el delito cibernético en los planos nacional e internacional y proponer otras nuevas.

2. La primera reunión del Grupo de Expertos se celebró en Viena del 17 al 21 de enero de 2011. En esa reunión, el Grupo de Expertos analizó y aprobó un conjunto de temas y una metodología para el estudio (E/CN.15/2011/19, anexos I y II).

3. La segunda reunión del Grupo de Expertos se celebró del 25 al 28 de febrero de 2013. En esa reunión, el Grupo de Expertos tomó nota del proyecto de estudio exhaustivo del problema del delito cibernético y las respuestas de los Estados Miembros, la comunidad internacional y el sector privado ante ese fenómeno, que había preparado la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) con las orientaciones del Grupo de Expertos, de conformidad con el mandato contenido en la resolución 65/230 de la Asamblea General, y tomó nota también del conjunto de temas que habrían de examinarse en un estudio exhaustivo de las consecuencias del delito

* E/CN.15/2018/1.

cibernético y la respuesta ante ese fenómeno y de la metodología que se emplearía para realizar el estudio, que se aprobaron en la primera reunión del Grupo de Expertos.

4. En la Declaración de Doha sobre la Integración de la Prevención del Delito y la Justicia Penal en el Marco Más Amplio del Programa de las Naciones Unidas para Abordar los Problemas Sociales y Económicos y Promover el Estado de Derecho a Nivel Nacional e Internacional y la Participación Pública, aprobada por el 13er Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal y que la Asamblea General hizo suya en su resolución 70/174, los Estados Miembros tomaron conocimiento de las actividades del Grupo de Expertos, la comunidad internacional y el sector privado, e invitaron a la Comisión a que estudiara la posibilidad de recomendar que el Grupo de Expertos, basándose en su propia labor, siguiera intercambiando información sobre legislación nacional, mejores prácticas, asistencia técnica y cooperación internacional, con miras a examinar opciones para fortalecer las actuales respuestas y proponer nuevas respuestas jurídicas o de otra índole frente al delito cibernético a nivel nacional e internacional.

5. La tercera reunión del Grupo de Expertos se celebró del 10 al 13 de abril de 2017. En esa reunión, el Grupo de Expertos aprobó los resúmenes del Relator sobre las deliberaciones de las reuniones 1ª y 2ª del Grupo de Expertos y examinó, entre otras cuestiones, un proyecto de estudio exhaustivo del problema del delito cibernético y las observaciones recibidas al respecto, y el modo de avanzar sobre la base del proyecto de estudio, e intercambió información sobre legislación nacional, mejores prácticas, asistencia técnica y cooperación internacional.

6. En su resolución 26/4, aprobada en su 26º período de sesiones, celebrado en mayo de 2017, la Comisión de Prevención del Delito y Justicia Penal solicitó al Grupo de Expertos que prosiguiera su labor y, para ello, celebrara reuniones periódicas y funcionara como plataforma para impulsar el debate sobre cuestiones sustantivas relacionadas con el delito cibernético, siguiendo la evolución de las tendencias al respecto, y en consonancia con la Declaración de Salvador y la Declaración de Doha, y solicitó también al Grupo de Expertos que siguiera intercambiando información sobre legislación nacional, mejores prácticas, asistencia técnica y cooperación internacional, con miras a examinar opciones para fortalecer las respuestas actuales y proponer nuevas respuestas jurídicas o de otra índole a nivel nacional e internacional frente al delito cibernético.

7. La Mesa ampliada decidió las fechas de la cuarta reunión del Grupo de Expertos mediante el procedimiento de acuerdo tácito el 23 de enero de 2018, y las confirmó en su reunión celebrada el 26 de enero de 2018.

II. Lista de recomendaciones y conclusiones preliminares

8. En consonancia con el programa de trabajo del Grupo de Expertos para el período 2018-2021, que el Grupo de Expertos aprobó en su primera sesión, celebrada el 3 de abril de 2018, el Relator, en cada reunión que celebre el Grupo de Expertos en 2018, 2019 y 2020, preparará con la asistencia de la Secretaría y con arreglo a los debates y deliberaciones del Grupo de Expertos, una lista de conclusiones y recomendaciones preliminares sugeridas por los Estados Miembros, que deberá ser concisa y centrarse en el fortalecimiento de las respuestas prácticas al delito cibernético. Como se especifica en el plan de trabajo, esa lista, en la que se recopilarán las sugerencias formuladas por los Estados Miembros, se incluirá en el informe de cada reunión para su posterior examen en la reunión que se celebre a más tardar en 2021 para hacer balance. También en consonancia con el plan de trabajo, en dicha reunión el Grupo de Expertos examinará las conclusiones y recomendaciones preliminares que se hayan recopilado, con el fin de elaborar una lista consolidada y amplia de las conclusiones y recomendaciones aprobadas para presentarla a la Comisión de Prevención del Delito y Justicia Penal.

A. Legislación y marcos

9. De conformidad con el plan de trabajo, 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 “Legislación y marcos”. 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.

a) Los Estados Miembros deberían velar por que sus disposiciones legislativas resistan el paso del tiempo frente a futuros avances tecnológicos promulgando leyes cuya formulación sea neutral tecnológicamente y que penalicen las actividades consideradas ilícitas en lugar de los medios utilizados. Asimismo, los Estados Miembros deberían considerar la posibilidad de adoptar una terminología coherente para describir las actividades cibernéticas delictivas y facilitar, en la medida de lo posible, una interpretación precisa de las leyes pertinentes por parte de los organismos encargados de hacer cumplir la ley y el poder judicial.

b) Los Estados Miembros deberían respetar los derechos soberanos de otros Estados en cuanto a la formulación de políticas y leyes que respondan a sus circunstancias y necesidades nacionales para hacer frente a la ciberdelincuencia. Para fomentar la cooperación internacional en la lucha contra el delito cibernético, el principio de la soberanía nacional no debería interpretarse erróneamente como un obstáculo, sino más bien considerarse fundamental y contemplarse como un punto de partida. El carácter inestable de la transmisión y el almacenamiento de datos electrónicos, por ejemplo, en las denominadas “nubes”, tal vez requiera entablar debates multilaterales sobre una asistencia recíproca innovadora y ampliada entre Estados, con miras a asegurar el acceso oportuno a datos y pruebas electrónicos.

c) Con el fin de prevenir y eliminar los refugios para los delincuentes, los Estados Miembros deberían cooperar entre sí en la mayor medida posible en la investigación, la reunión de pruebas, el enjuiciamiento, el fallo y, en caso necesario, la eliminación de contenidos ilícitos de Internet. Los Estados Miembros también deberían ofrecer la máxima flexibilidad posible al cooperar a nivel internacional para combatir la ciberdelincuencia y otros delitos que entrañen datos electrónicos, ya sea al liderar investigaciones o al compartir pruebas, independientemente de que las actividades subyacentes tengan denominaciones distintas en los respectivos Estados. Al hacerlo, los Estados Miembros deberían tener presente que, por lo general, la doble incriminación es requisito para extraditar, pero no necesariamente para prestar asistencia judicial recíproca.

d) Al formular políticas y leyes, los Estados Miembros deberían tener en cuenta la necesidad de lograr un equilibrio entre, por una parte, la protección de los derechos humanos y, por otra, la seguridad nacional, el orden público y los derechos legítimos de terceros. Las legislaciones nacionales que penalizan conductas asociadas con la ciberdelincuencia y otorgan autoridad procesal para la investigación, el enjuiciamiento y el fallo de casos de delitos cibernéticos deberían respetar las garantías procesales, el derecho a la intimidad, las libertades civiles y los derechos humanos. Las políticas y leyes nacionales, así como los instrumentos internacionales existentes o los que se elaboren en el futuro, deberían adoptar un enfoque multidimensional. Por un lado, deberían incluir políticas adecuadas en materia de ciberdelincuencia basadas en una comprensión amplia del concepto general de ciberseguridad. Por otro lado, no solo deberían abarcar la conducta ilícita, sino también centrarse en la prevención del delito y la prestación de asistencia a las víctimas y a la población en general. Con miras a crear una base sólida para la cooperación internacional en la lucha contra la ciberdelincuencia, los Estados Miembros deberían esforzarse por lograr y promover una cultura que fomente la creación de un futuro común para el ciberespacio.

e) Los Estados Miembros deberían cooperar a nivel internacional sin exigir la plena armonía de las legislaciones nacionales, siempre que la conducta subyacente esté tipificada como delito y las leyes sean lo suficientemente compatibles para simplificar y agilizar las distintas formas de cooperación.

f) Los Estados Miembros deberían tener en cuenta que los marcos jurídicos nacionales siguen siendo decisivos para asegurar la eficacia y el equilibrio general del sistema de investigación y enjuiciamiento, dado que el derecho penal tiene particularmente en cuenta los derechos fundamentales, y las investigaciones de los delitos informáticos atañen en gran medida a las comunicaciones privadas y los datos de los ciudadanos.

g) A fin de facilitar el enjuiciamiento de los actos delictivos, los Estados Miembros deberían legislar acerca de la jurisdicción extraterritorial respecto de los nacionales y las personas que tengan residencia habitual en su territorio, independientemente del lugar en que se cometieran los actos y de si constituyen delito en la jurisdicción extranjera.

h) Los Estados Miembros pueden utilizar diferentes bases jurídicas para cooperar a nivel internacional, incluida la reciprocidad, los tratados bilaterales o multilaterales y otros acuerdos. Además, los Estados Miembros con capacidades e infraestructura más avanzadas en el ámbito de la ciberdelincuencia, al prestar asistencia jurídica a otros Estados, deberían asumir responsabilidades proporcionales a las capacidades o la infraestructura que poseen.

i) Con el fin de que las cuestiones pertinentes se tengan en cuenta debidamente, los Estados Miembros deberían celebrar consultas con todos los interesados correspondientes, incluidos los interesados intergubernamentales, el sector privado y la sociedad civil, tan pronto como sea posible una vez se haya decidido introducir legislación contra el delito cibernético.

j) Los Estados Miembros deberían promover una cooperación sólida y basada en la confianza entre los sectores público y privado en el ámbito de la ciberdelincuencia, incluida la cooperación entre las autoridades encargadas de hacer cumplir la ley y los proveedores de servicios de comunicaciones. Para fortalecer y facilitar la cooperación también es necesario entablar un diálogo con el sector privado, además de establecer alianzas público-privadas en la medida de lo posible y concertar memorandos de entendimiento en caso necesario.

k) Los Estados Miembros deberían apoyar a la UNODC en la creación de un proyecto o programa educativo destinado a concienciar sobre la ciberdelincuencia y las respuestas apropiadas a ese fenómeno entre las autoridades judiciales y fiscales, los expertos en ciencia forense digital de los Estados Miembros y las entidades privadas, y utilizar instrumentos de creación de capacidad o una plataforma electrónica de gestión de los conocimientos con el fin de sensibilizar a la sociedad civil sobre las repercusiones de la ciberdelincuencia.

l) La elaboración, promulgación y aplicación eficaces de leyes nacionales para combatir el delito cibernético deberían estar respaldadas por medidas de creación de capacidad y programas de asistencia técnica. Los Estados Miembros deberían asignar recursos suficientes para fomentar la capacidad interna. Para aplicar adecuadamente la legislación contra la ciberdelincuencia es necesario capacitar a los policías y los fiscales, así como realizar campañas de sensibilización pública. Esos recursos también fomentarán la cooperación internacional, ya que esta se ve reforzada por la capacidad interna de los países para investigar y enjuiciar los delitos relacionados con la ciberdelincuencia.

m) Los Estados Miembros deberían fortalecer los marcos y redes existentes de lucha contra la ciberdelincuencia determinando y examinando los puntos débiles de esos marcos y redes y proporcionando los recursos necesarios para mejorar su eficacia.

n) La UNODC debería participar activamente en el fomento de la capacidad de todos los Estados Miembros que necesiten asistencia, en particular los países en desarrollo. Las actividades de creación de capacidad deberían ser neutrales desde el punto de vista político, no estar condicionadas, ser el resultado de consultas exhaustivas y ser aceptadas voluntariamente por los países receptores. En cuanto al fondo, esas actividades deberían abarcar al menos los siguientes ámbitos:

i) capacitación de jueces, fiscales, investigadores y autoridades encargadas de hacer cumplir la ley con respecto a la investigación de delitos cibernéticos, la gestión de pruebas electrónicas, la cadena de custodia y el análisis forense;

ii) redacción, modificación o aplicación de leyes en materia de ciberdelincuencia y pruebas electrónicas;

iii) estructuración de dependencias de investigación de la ciberdelincuencia y orientación sobre procesos conexos;

iv) redacción, actualización y aplicación de leyes contra el uso de Internet con fines terroristas.

o) La UNODC debería buscar sinergias y cooperar estrechamente con otros interesados u organizaciones como el Consejo de Europa y la Organización de los Estados Americanos (OEA) en relación con programas de creación de capacidad en materia de lucha contra la ciberdelincuencia, con miras a evitar la dispersión o fragmentación de las actividades e iniciativas en esa esfera.

p) Los Estados Miembros deberían seguir utilizando el Grupo de Expertos como plataforma para intercambiar información y mejores prácticas, incluidas leyes modelo o cláusulas modelo, respecto de cuestiones como la jurisdicción, las técnicas especiales de investigación, las pruebas electrónicas (en particular los desafíos planteados por su carácter inestable y su admisibilidad en los tribunales) y la cooperación internacional.

q) A fin de evitar la fragmentación, los Estados Miembros deberían examinar prácticas y normas aceptadas universalmente, celebrando consultas multilaterales bajo los auspicios de las Naciones Unidas y por conducto de la plataforma del Grupo de Expertos.

r) Los Estados Miembros deberían evaluar la posibilidad y viabilidad de otorgar al Grupo de Expertos o a la UNODC el mandato de realizar y publicar periódicamente, con contribuciones sustantivas de los Estados Miembros, una evaluación de las tendencias de la ciberdelincuencia.

s) Los Estados Miembros deberían elaborar, en el marco de las Naciones Unidas, un nuevo instrumento jurídico internacional sobre ciberdelincuencia que atienda las preocupaciones y los intereses de todos los Estados Miembros.

t) Los Estados Miembros deberían utilizar o adherirse a los instrumentos jurídicos multilaterales vigentes contra el delito cibernético, como el Convenio sobre la Ciberdelincuencia (Convenio de Budapest) del Consejo de Europa, ya que muchos Estados los toman como modelos de mejores prácticas a partir de los cuales se pueden formular respuestas nacionales e internacionales adecuadas ante ese fenómeno.

u) Los instrumentos y mecanismos jurídicos existentes, incluida la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, deberían ser aprovechados por el mayor número posible de Estados, a fin de fortalecer la cooperación internacional.

v) Bajo los auspicios del Grupo de Expertos, los Estados Miembros deberían explorar respuestas aplicables a nivel internacional que pudieran reflejarse en leyes modelo o cláusulas modelo, en su caso, y para ello deberían basarse en las mejores prácticas contenidas en los instrumentos regionales o en la legislación nacional existentes.

B. Tipificación

10. De conformidad con el plan de trabajo, el presente párrafo contiene una recopilación de las sugerencias formuladas por los Estados Miembros en la reunión en relación con el tema 3 del programa, titulado “Tipificación”. 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.

a) Los Estados Miembros deberían tener en cuenta que muchas disposiciones sustantivas del derecho penal concebidas para los delitos no cometidos en línea también pueden ser aplicables a los delitos cometidos en línea. Por lo tanto, para fortalecer la aplicación de la ley, los Estados Miembros deberían utilizar las disposiciones vigentes del derecho nacional e internacional, según proceda, para hacer frente a la delincuencia en el entorno en línea.

b) Los Estados Miembros deberían aprobar y aplicar leyes nacionales para penalizar las actividades cibernéticas ilícitas y otorgar autoridad procesal a los organismos encargados de hacer cumplir la ley para investigar los presuntos delitos respetando las garantías procesales, el derecho a la intimidad, las libertades civiles y los derechos humanos.

c) Los Estados Miembros deberían seguir promulgando legislación penal relativa específicamente a la ciberdelincuencia que tenga en cuenta las nuevas conductas delictivas asociadas al uso indebido de la tecnología de la información y las comunicaciones, a fin de no tener que recurrir a las disposiciones del derecho penal aplicables de manera general.

d) Los Estados Miembros deberían tipificar los delitos cibernéticos básicos que afectan a la confidencialidad, la integridad y la disponibilidad de las redes de computadoras y los datos informáticos, teniendo en cuenta las normas internacionales reconocidas ampliamente.

e) Los actos cibernéticos considerados infracciones leves y no delitos deberían tratarse en reglamentos civiles y administrativos en lugar de en la legislación penal.

f) En la medida en que aún no lo hayan hecho, los Estados Miembros deberían considerar la posibilidad de tipificar como delito las siguientes conductas:

i) las formas de actividad cibernética delictiva nuevas y emergentes, como el uso indebido delictivo de criptomonedas, los delitos cometidos en la web oscura y la Internet de las cosas, el *phishing*, y la distribución de programas maliciosos y otros programas informáticos utilizados para cometer actos delictivos;

ii) la divulgación de información personal y la “pornovenganza”;

iii) el uso de Internet para cometer actos relacionados con el terrorismo;

iv) el uso de Internet para incitar a cometer delitos motivados por prejuicios y al extremismo violento;

v) la prestación de apoyo técnico o asistencia para la comisión de un acto cibernético delictivo;

vi) la creación de plataformas en línea ilícitas o la publicación de información para cometer delitos cibernéticos;

vii) la obtención de acceso por medios ilícitos a sistemas informáticos o la piratería de dichos sistemas;

viii) la interceptación o el daño ilícitos de datos informáticos y el daño ilícito a sistemas informáticos;

ix) la interferencia ilícita en los datos y sistemas informáticos;

x) el uso indebido de dispositivos;

xi) la falsificación y el fraude informáticos;

xii) el abuso y explotación sexuales de menores;

xiii) la infracción de la propiedad intelectual;

xiv) el abuso y explotación sexuales de menores, y la inducción de menores al suicidio;

xv) la influencia ilícita sobre infraestructuras de información esenciales.

g) Los Estados Miembros deberían garantizar que los delitos relacionados específicamente con la informática se tipifiquen en disposiciones hechas a medida que no se limiten a ampliar el ámbito de aplicación de los delitos tradicionales al entorno digital, sino que tengan en cuenta las particularidades de ese entorno y la necesidad real de tipificación basada en una evaluación cuidadosa.

h) Los Estados Miembros deberían tener en cuenta que la armonización internacional de la tipificación de la ciberdelincuencia debería centrarse en un conjunto básico de delitos contra la confidencialidad, la integridad y la accesibilidad de los sistemas de información, mientras que la necesidad de armonizar la tipificación relativa a los delitos generales cometidos mediante el uso de tecnología de la información y las comunicaciones debería tratarse principalmente en foros especializados sobre las distintas esferas concretas de la delincuencia.

i) Los Estados Miembros deberían evitar tipificar como delitos una amplia gama de actividades realizadas por proveedores de servicios de Internet (PSI), especialmente cuando esas normas puedan limitar indebidamente la libertad de expresión y la expresión de ideas y creencias. Más bien deberían trabajar con los PSI y el sector privado para fortalecer la cooperación con las autoridades encargadas de hacer cumplir la ley, observando en particular que la mayoría de los PSI tienen un gran interés en asegurar que sus plataformas no sean objeto de abuso por parte de delincuentes.

j) Los Estados Miembros deberían aprobar y aplicar marcos jurídicos nacionales relativos a las pruebas para permitir que las pruebas electrónicas se admitan en investigaciones y enjuiciamientos penales, incluida la compartición adecuada de pruebas electrónicas con asociados extranjeros encargados de hacer cumplir la ley.

k) Los Estados Miembros deberían utilizar la Convención contra la Delincuencia Organizada para facilitar la compartición de información y pruebas para las investigaciones penales de delitos cibernéticos, dada la frecuente participación de grupos delictivos organizados en ese tipo de actividad delictiva.

l) Los Estados Miembros deberían estudiar formas de ayudar a garantizar que el intercambio de información entre investigadores y fiscales que afrontan la ciberdelincuencia sea oportuno y seguro, en particular reforzando las redes de instituciones nacionales que puedan estar disponibles las 24 horas.

m) En cuanto a la cuestión de tipificar el incumplimiento por parte de los PSI de lo solicitado por los organismos encargados de hacer cumplir la ley, los Estados Miembros deberían actuar con cautela y examinar minuciosamente los perjuicios para las actividades del sector privado y los derechos humanos fundamentales, en particular la libertad de expresión.

n) Para afrontar eficazmente la ciberdelincuencia, los Estados Miembros deberían tomar en consideración los marcos de derechos humanos existentes, en particular en lo que se refiere a la libertad de expresión y el derecho a la intimidad, y respetar los principios de legalidad, necesidad y proporcionalidad en los procesos penales relativos a la lucha contra el delito cibernético.

o) Los Estados Miembros deberían llevar a cabo investigaciones para determinar las tendencias de las actividades que subyacen al ciberdelito y deberían seguir evaluando la posibilidad y viabilidad de otorgar al Grupo de Expertos o a la UNODC el mandato de realizar y publicar anualmente, con contribuciones sustantivas de los Estados Miembros, una evaluación de las tendencias de la ciberdelincuencia.

p) Los Estados Miembros deberían estudiar la posibilidad de aprobar estrategias amplias de lucha contra la ciberdelincuencia que incluyan la elaboración de estudios sobre victimización y la realización de actividades para informar y empoderar a las víctimas potenciales de la ciberdelincuencia.

q) Los Estados Miembros deberían considerar la posibilidad de adoptar nuevas medidas preventivas contra la ciberdelincuencia, en particular, aunque no

exclusivamente, medidas para el uso responsable de Internet, especialmente por parte de los niños y los jóvenes.

III. Resumen de las deliberaciones

A. Aprobación del plan de trabajo del Grupo de Expertos propuesto por la Presidencia para el período 2018-2021

11. En su primera sesión, celebrada el 3 de abril de 2018, el Grupo de Expertos examinó el tema 1 c) del programa, titulado “Aprobación del programa de trabajo del Grupo de Expertos propuesto por la Presidencia para el período 2018-2021”. El programa de trabajo del Grupo de Expertos propuesto por la Presidencia para el período 2018-2021 fue aprobado.

B. Legislación y marcos

12. En sus sesiones 2ª a 4ª, celebradas los días 3 y 4 de abril de 2018, el Grupo de Expertos examinó el tema 2 del programa, titulado “Legislación y marcos”.

13. Facilitaron el examen los siguientes panelistas: Lu Chuanying (China); George Maria Tyendezwa (Nigeria); Cristina Schulman (Rumania); Pedro Verdelho (Portugal); Claudio Peguero (República Dominicana); María Alejandra Daglio (Argentina); y Mohamed Mghari (Marruecos).

14. En el debate celebrado a continuación, muchas delegaciones hicieron referencia a las novedades legislativas y en materia de políticas de sus países en lo que respectaba al delito cibernético y la ciberseguridad. Hicieron hincapié en el papel fundamental que desempeñaban los programas de creación de capacidad y asistencia técnica en apoyo de la aplicación eficaz de la legislación nacional y el fomento de la capacidad nacional para la investigación, el enjuiciamiento y el fallo, así como la cooperación internacional. También se destacó la necesidad de aplicar enfoques multidisciplinarios en los que participaran la sociedad civil y el sector privado.

15. Varios oradores opinaron que no se necesitaba un nuevo instrumento jurídico amplio a nivel mundial para afrontar el delito cibernético, puesto que consideraban que los instrumentos internacionales ya existentes, como el Convenio de Budapest y la Convención contra la Delincuencia Organizada, eran suficientes para elaborar respuestas adecuadas de cooperación a nivel nacional e internacional ante el delito cibernético. Según esos oradores, el Convenio de Budapest ofrecía a los Estados partes (entre los que figuraban varios Estados que no eran miembros del Consejo de Europa) y a los Estados que lo utilizaban como referencia un marco jurídico y operacional eficaz para hacer frente a la ciberdelincuencia transfronteriza porque, entre otras cosas, facilitaba la cooperación internacional y la armonización de las disposiciones pertinentes del derecho penal y de procedimiento penal. También se hizo referencia a la labor del Comité del Convenio sobre la Ciberdelincuencia y a los proyectos de creación de capacidad del Consejo de Europa en apoyo de la aplicación del Convenio, como el proyecto ampliado Acción Global contra la Ciberdelincuencia, y otros proyectos de divulgación que incluían la prestación de asistencia técnica, por ejemplo en el marco de la OEA y la Comunidad Económica de los Estados del África Occidental. Además, se afirmó que las negociaciones relativas a un nuevo tratado supondrían demasiado tiempo y recursos debido a la falta de consenso sobre aspectos fundamentales como el ámbito de aplicación, la soberanía nacional y la jurisdicción, lo que podría repercutir en la aprobación por parte de los Estados de normas adecuadas para combatir la ciberdelincuencia.

16. Otros oradores reiteraron su opinión de que se precisaban respuestas nuevas, incluido un nuevo instrumento jurídico universal o global sobre ciberdelincuencia en el marco de las Naciones Unidas, para hacer frente a los desafíos planteados por el rápido desarrollo de la tecnología de Internet que no se abordaban en los mecanismos vigentes.

Se expresó la opinión de que los mecanismos existentes no deberían impedir que se debatiera a nivel internacional la elaboración de respuestas nuevas. Algunos oradores consideraban que el Convenio de Budapest era un instrumento jurídico regional que no atendía las preocupaciones de todos los Estados Miembros. Algunos oradores mostraron su preocupación por el carácter cerrado del proceso de adhesión, puesto que únicamente se podían adherir Estados al Convenio por invitación y previa aprobación de los Estados partes. Un orador sugirió que una posibilidad jurídica eficaz para la cooperación entre los Estados que no eran partes en el Convenio de Budapest era el proyecto de convención de las Naciones Unidas sobre cooperación en la lucha contra la ciberdelincuencia que se presentó al Secretario General el 11 de octubre de 2017 (A/C.3/72/12, anexo).

17. Varios oradores recordaron que todo instrumento debía incluir normas y salvaguardias adecuadas para proteger los derechos humanos básicos.

18. Algunos oradores opinaron que el Convenio de Budapest, en particular su artículo 32, apartado b), planteaba obstáculos para el derecho internacional que eran difíciles de aceptar, como el respeto de la soberanía nacional. Otros oradores señalaron que el alcance del artículo 32, apartado b), era limitado y que algunos Estados sobrepasaban actualmente esa disposición sin las salvaguardias procesales que se aplicaban a todos los artículos del Convenio de Budapest.

19. Algunos oradores consideraban que la Convención contra la Delincuencia Organizada era pertinente para la lucha contra el delito cibernético, dado que era un fenómeno cada vez más transnacional y que, en muchos casos, estaba relacionado con la delincuencia organizada.

20. El Grupo de Expertos también examinó la relación y las diferencias entre la ciberseguridad y la ciberdelincuencia. Varios oradores indicaron que se trataba de dos conceptos diferentes dentro de los amplísimos retos que planteaba el uso de la tecnología moderna de la información y las comunicaciones y que, por ese motivo, debían examinarse en foros de las Naciones Unidas diferentes y más apropiados, como la Unión Internacional de Telecomunicaciones o el Grupo de Expertos Gubernamentales en Seguridad de la Información. No obstante, varios oradores señalaron que esos temas estaban interrelacionados debido a que, en la práctica, era necesario examinar las cuestiones relativas a la ciberseguridad a fin de combatir eficazmente el delito cibernético. Se hizo un llamamiento en favor de una cooperación más estrecha y de acuerdos con el sector privado.

21. Muchos oradores agradecieron la labor que realizaba la UNODC por conducto del Programa Mundial contra el Delito Cibernético y ofrecieron ejemplos de actividades de asistencia técnica y creación de capacidad que se habían llevado a cabo en sus países o regiones en el marco del Programa. Varios oradores también señalaron que otras organizaciones intergubernamentales de sus regiones, como la Comunidad de Estados Independientes, la OEA, la Unión Africana, la Organización de Cooperación de Shanghái y el Consejo de Europa, también prestaban asistencia legislativa y de otra índole para combatir el delito cibernético.

22. Los oradores agradecieron la labor que habían desempeñado la Presidencia y la Mesa del Grupo de Expertos, así como la Secretaría, para organizar la reunión. Muchos oradores expresaron apoyo a la labor del Grupo de Expertos. Algunos oradores señalaron que era un foro valioso en el que expertos de diversas jurisdicciones podían mantener conversaciones multilaterales. Según algunos oradores, el Grupo de Expertos podía resultar eficaz en el examen de respuestas a las amenazas comunes que planteaba el delito cibernético, lo que incluía atender las necesidades de los países en materia de asistencia técnica y creación de capacidad. Se acogió favorablemente el hecho de que el Grupo de Expertos hubiera aprobado su programa de trabajo para el período 2018-2021, que se consideró un paso en la dirección correcta.

23. En su tercera sesión, el Grupo de Expertos siguió examinando el tema 2 del programa. Los oradores plantearon otras cuestiones, en particular la importancia de velar por que en la legislación relativa al delito cibernético y los acuerdos o arreglos de cooperación internacional, especialmente los relativos a pruebas electrónicas, se respetaran las salvaguardias relativas a los derechos humanos consagradas en el

derecho y las normas internacionales. En concreto, se señaló la importancia de lograr un equilibrio entre, por una parte, los derechos a la intimidad y la libertad de expresión y, por otra parte, la necesidad de prevenir y combatir la ciberdelincuencia. Varios oradores observaron un mayor grado de convergencia en la tipificación de los delitos relacionados con la ciberdelincuencia en distintas jurisdicciones, lo que contribuía a reducir la fragmentación de las normas jurídicas en ese ámbito. Otros desafíos pendientes eran el mayor fortalecimiento de la cooperación internacional mediante prácticas de cooperación tanto oficiales como oficiosas y las cuestiones jurisdiccionales que planteaba la computación en la nube.

24. El Grupo de Expertos examinó también el acceso transfronterizo a los datos. Se expresó la opinión de que las deliberaciones sobre esa cuestión en el contexto del Grupo de Expertos y en otros foros intergubernamentales pertinentes habían sido muy útiles para determinar mejores prácticas y estrechar la cooperación entre jurisdicciones para la investigación de los delitos cibernéticos. El respeto del principio de la soberanía nacional era una cuestión que debía examinarse más a fondo, pues no siempre quedaba claro cómo las prácticas para acceder a datos ubicados en otras jurisdicciones eran compatibles con ese principio. Se puso de relieve asimismo el principio de proporcionalidad en los esfuerzos por frenar la ciberdelincuencia. Según muchos oradores, en la legislación contra el delito cibernético se debía utilizar un lenguaje tecnológicamente neutro que no fuera a quedar desfasado respecto al ritmo del desarrollo tecnológico y de las tendencias delictivas, pero que fuera suficientemente concreto para reflejar las principales actividades delictivas. Varios oradores pusieron de relieve la necesidad de hacer frente y responder al creciente uso de Internet con fines terroristas y para difundir discursos de odio y noticias falsas, mediante la creación de legislación nacional o su actualización. Se consideró que los marcos jurídicos se aplicarían más eficazmente si iban acompañados de proyectos de asistencia técnica y creación de capacidad.

C. Tipificación

25. En sus sesiones 4ª y 5ª, celebradas los días 4 y 5 de abril de 2018, el Grupo de Expertos examinó el tema 3 del programa titulado “Tipificación”.

26. Facilitaron el examen los siguientes panelistas: Malini Govender (Sudáfrica), Li Jingjing (China), Vadim Sushchik (Federación de Rusia), Eric do Val Lacerda Sogocio (Brasil), Marouane Hejjouji (Marruecos) y Normand Wong (Canadá).

27. Muchos oradores proporcionaron información sobre la forma en que sus países tipificaban los delitos cibernéticos. Entre los delitos más comunes que mencionaron los oradores figuraban delitos específicamente cibernéticos, denominados a menudo delitos cibernéticos básicos, como los cometidos contra la confidencialidad, la integridad y la accesibilidad de los sistemas informáticos, así como delitos propiciados por medios cibernéticos, incluidos los delitos relacionados con el abuso y la explotación de menores, los delitos contra la intimidad, los delitos relativos a los datos personales y el uso de Internet con fines terroristas. Los oradores señalaron que la mayoría de los países ya contaban con legislación que tipificaba los delitos cibernéticos básicos. Los oradores observaron que, para cumplir el principio de la doble incriminación y eliminar los refugios para los delincuentes, no era necesario que los Estados tuvieran la misma tipología de los delitos, siempre que la conducta subyacente constituyera delito en todas las jurisdicciones.

28. Los oradores también pusieron de relieve la necesidad de legislación sobre la admisibilidad de pruebas electrónicas en investigaciones y enjuiciamientos penales para luchar eficazmente contra la ciberdelincuencia. La introducción de legislación de ese tipo debía complementarse con actividades adecuadas de capacitación y creación de capacidad para los funcionarios encargados de hacer cumplir la ley, los fiscales y los jueces. También se destacó la importancia de que las jurisdicciones compartieran pruebas electrónicas.

29. Los oradores expusieron las experiencias de sus países en cuanto a la elaboración de legislación y leyes para tipificar las actividades de ciberdelincuencia. Los expertos hablaron sobre los casos en que era necesario crear legislación específica nueva para tipificar como delitos ciertos actos y aquellos en que la legislación y los delitos generales existentes bastaban y eran adecuados para combatir las formas del delito cibernético nuevas y emergentes. Muchos oradores consideraron muy útil que la legislación se mantuviera neutra desde el punto de vista tecnológico, de forma que pudiera seguir siendo aplicable cuando sugieran nuevas formas de tecnología de la información y las comunicaciones y de delitos cibernéticos. Cada país tenía necesidades diferentes y podía examinar si era necesario tipificar nuevos delitos en función de las tendencias delictivas a que se enfrentara. Los oradores también señalaron la necesidad de disponer de legislación adecuada para tipificar nuevas formas de delincuencia impulsadas por el uso indebido delictivo de, entre otras cosas, las criptomonedas, la Internet de las cosas y la web oscura.

30. El Grupo de Expertos examinó cuestiones relacionadas con las sanciones a los PSI que no cooperasen con los organismos de aplicación de la ley o no cumplieran los requisitos legales para la prevención de la ciberdelincuencia. El Grupo de Expertos examinó también la forma en que el sector privado podía cooperar con los organismos encargados de hacer cumplir la ley sobre la base de las mejores prácticas que se hubieran determinado con respecto a las responsabilidades jurídicas y la rendición de cuentas de los PSI. Otros oradores observaron que, al mismo tiempo, era importante tener en cuenta las salvaguardias relativas a los derechos humanos al exigir el cumplimiento por parte de los PSI. Se planteó la cuestión de si la responsabilidad de los PSI debía incluirse en el ámbito de las medidas de tipificación.

31. Respecto de la prevención de la ciberdelincuencia, varios oradores subrayaron la importancia de elaborar campañas de concienciación para el público en general, así como programas de educación específicos para los niños con el fin de informarlos acerca de los riesgos de la ciberdelincuencia y mejorar la seguridad en línea y la ciberseguridad en todo el país. Además, se precisaban cursos de capacitación a medida y la asignación de los recursos necesarios a fin de aumentar la capacidad de los organismos encargados de hacer cumplir la ley para prevenir la ciberdelincuencia.

IV. Organización de la reunión

A. Apertura de la reunión

32. Declaró abierta la sesión el Sr. André Rypl (Brasil), Vicepresidente del Grupo de Expertos, en su calidad de Presidente de la cuarta reunión del Grupo de Expertos.

B. Declaraciones

33. Formularon declaraciones expertos de los siguientes Estados: Albania, Alemania, Argelia, Argentina, Australia, Belarús, Bosnia y Herzegovina, Brasil, Bulgaria, Canadá, Chequia, Chile, China, Colombia, Costa Rica, Ecuador, Egipto, El Salvador, Estados Unidos de América, Estonia, ex República Yugoslava de Macedonia, Federación de Rusia, Filipinas, Georgia, Ghana, Guatemala, India, Indonesia, Irán (República Islámica del), Italia, Japón, Jordania, Kazajstán, Kuwait, Liechtenstein, Malasia, Mauricio, México, Montenegro, Nigeria, Noruega, Países Bajos, Paraguay, Portugal, Reino Unido de Gran Bretaña e Irlanda del Norte, República Dominicana, República de Moldova, Rumania, Serbia, Sri Lanka, Sudáfrica, Tailandia, Túnez, Turquía, Ucrania y Viet Nam.

34. Formularon declaraciones también los representantes de las siguientes organizaciones intergubernamentales: Consejo de Europa, Organización de Cooperación de Shanghái y Unión Europea.

C. Aprobación del programa y otras cuestiones de organización

35. En su primera sesión, celebrada el 3 de abril de 2018, el Grupo de Expertos aprobó el siguiente programa provisional:

1. Cuestiones de organización:
   a) Apertura de la reunión;
   b) Aprobación del programa;
   c) Aprobación del programa de trabajo del Grupo de Expertos propuesto por la Presidencia para el período 2018-2021.
2. Legislación y marcos.
3. Tipificación.
4. Otros asuntos.
5. Aprobación del informe.

D. Asistencia

36. Asistieron a la reunión representantes de 98 Estados Miembros, 1 Estado observador, 1 dependencia de la Secretaría de las Naciones Unidas, 4 organizaciones intergubernamentales y 9 instituciones en representación del mundo académico y el sector privado.

37. En la reunión se distribuyó una lista provisional de participantes (UNODC/CCPCJ/EG.4/2018/INF/1).

E. Documentación

38. Además del proyecto de estudio exhaustivo del problema del delito cibernético y las respuestas de los Estados Miembros, la comunidad internacional y el sector privado ante ese fenómeno, el Grupo de Expertos tuvo ante sí los siguientes documentos:

a) Programa provisional (UNODC/CCPCJ/EG.4/2018/1);

b) Plan de trabajo del Grupo de Expertos propuesto por la Presidencia para el período 2018-2021, basado en la resolución 26/4 de la Comisión de Prevención del Delito y Justicia Penal (UNODC/CCPCJ/EG.4/2018/CRP.1).

V. Aprobación del informe

39. En su sexta sesión, celebrada el 5 de abril de 2018, el Grupo de Expertos aprobó su informe (UNODC/CCPCJ/EG.4/2018/L.1).