Distr. general
12 de abril de 2019
Español
Original: inglés

Informe de la reunión del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético celebrada en Viena del 27 al 29 de marzo de 2019

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.

2. La primera reunión del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético 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 en Viena del 25 al 28 de febrero de 2013. En esa reunión, el Grupo de Expertos tomó nota del 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 la orientación del Grupo de Expertos, de conformidad con el mandato contenido en la resolución 65/230 de la Asamblea General y el conjunto de temas y la metodología para la realización del estudio que se aprobaron en la primera reunión del Grupo de Expertos. Se expresaron distintas opiniones sobre el contenido, las conclusiones y las opciones presentadas en el estudio (véase UNODC/CCPCJ/EG.4/2013/3).

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 refrendada por la Asamblea General en su resolución 70/174, los Estados Miembros tomaron conocimiento de las actividades del Grupo de Expertos e invitaron a la Comisión de

Prevención del Delito y Justicia Penal 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 en Viena del 10 al 13 de abril de 2017. En esa reunión, el Grupo de Expertos examinó, entre otras cosas, la posibilidad de aprobar los resúmenes del Relator sobre las deliberaciones de las reuniones primera y segunda del Grupo de Expertos, el proyecto de estudio exhaustivo del problema del delito cibernético y las observaciones recibidas al respecto, y el modo de avanzar con respecto al proyecto de estudio. También 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 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. También en esa resolución, la Comisión solicitó 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 frente al delito cibernético a nivel nacional e internacional.

7. La cuarta reunión del Grupo de Expertos se celebró en Viena del 3 al 5 de abril de 2018. En esa reunión, la labor del Grupo de Expertos se centró en la legislación y los marcos, así como en la tipificación en relación con el delito cibernético. Se examinaron las novedades legislativas y de políticas para hacer frente al delito cibernético a nivel nacional e internacional y se estudiaron las formas en que se tipificaba la ciberdelincuencia a nivel nacional. El Grupo de Expertos también aprobó el programa de trabajo propuesto para él por la Presidencia para el período 2018-2021 (UNODC/CCPCJ/EG.4/2018/CRP.1).

8. En la reunión que celebró el 2 de noviembre de 2018, la Mesa ampliada decidió la fecha de celebración de la quinta reunión del Grupo de Expertos y llegó a un acuerdo sobre el programa provisional.

II. Lista de recomendaciones y conclusiones preliminares

9. En consonancia con el programa de trabajo del Grupo de Expertos para el período 2018-2021, el Relator, en cada reunión que celebre el Grupo de Expertos en 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. Conforme al 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. Como se especifica en el plan de trabajo, en dicha reunión el Grupo de Expertos examinará la recopilación de conclusiones y recomendaciones preliminares y las compilará en una lista de conclusiones y recomendaciones aprobadas que se presentará a la Comisión. Antes de la reunión para hacer balance, las conclusiones y recomendaciones preliminares propuestas por los Estados Miembros se distribuirán a todos los Estados Miembros, observadores y otras partes interesadas para que formulen observaciones, las cuales se publicarán en línea con anterioridad a dicha reunión para que las examinen las delegaciones.

A. Aplicación de la ley e investigaciones

10. 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; tampoco están presentadas en orden de importancia:

a) Algunos Estados Miembros sugirieron que, debido a la naturaleza evolutiva, complicada y transnacional de la ciberdelincuencia, sería prematuro examinar normas comunes de cooperación internacional. Por consiguiente, los Estados Miembros deberían articular 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. Ese instrumento debería examinarse teniendo en cuenta, entre otras cosas, las preocupaciones e intereses de todos los Estados Miembros y 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) Sin embargo, otros Estados Miembros propusieron que no era ni necesario ni apropiado considerar la posibilidad de un nuevo instrumento jurídico 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 del Consejo de Europa sobre la Ciberdelincuencia (Convenio de Budapest). Sobre la base de esa 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 consideran 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 relacionada con 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 de los agentes de policía en la investigación del delito cibernético mediante actividades de capacitación, que imparten numerosos países, así como la UNODC y otros asociados, y que tiene por objeto fortalecer la capacidad de detección, investigación y lucha contra la ciberdelincuencia. Las actividades de creación de capacidad en esa esfera deberían atender, en particular, las necesidades de los países en desarrollo, centrarse en las vulnerabilidades de cada país a fin de prestar una asistencia técnica adaptada a sus necesidades y promover el intercambio de los conocimientos más actualizados 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 ese ámbito;

g) Los países deberían destinar recursos a generar los conocimientos especializados necesarios para investigar la ciberdelincuencia y establecer alianzas que se valgan de mecanismos de cooperación para obtener pruebas vitales;

h) Los Estados Miembros deberían seguir esforzándose por crear y apoyar dependencias, órganos y 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 las actuaciones penales;

i) En vista de que la lucha contra la ciberdelincuencia exige estrategias de aplicación de la ley a mediano y largo plazo para desmantelar los mercados de la ciberdelincuencia, que incluyan iniciativas de cooperación con los asociados internacionales, 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 promulgando leyes de carácter sustantivo sobre las formas nuevas y emergentes de delincuencia en el ciberespacio, con un lenguaje tecnológicamente neutro a fin de 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 seguir el ritmo de los avances tecnológicos y asegurar que los organismos encargados de hacer cumplir la ley dispongan de medios adecuados para combatir la delincuencia en línea. Deberían redactarse leyes pertinentes teniendo en cuenta los conceptos técnicos aplicables y 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 que autoricen 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 su posible inestabilidad;

ii) el registro y la incautación de los contenidos almacenadod en dispositivos digitales, que suelen ser las pruebas de la comisión de un delito electrónico más importantes;

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

v) la cooperación internacional de las autoridades nacionales encargadas de hacer cumplir la ley;

l) Dado que las investigaciones de delitos cibernéticos requieren creatividad, ingenio técnico y esfuerzos conjuntos entre los fiscales y la policía, los países deberían alentar una estrecha cooperación 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 que a la ubicación de los datos;

p) Los países deberían realizar una mayor labor de concienciación sobre la ciberdelincuencia entre el público en general y la industria privada a fin de aumentar la tasa de denuncia de delitos cibernéticos en comparación con otros tipos de delitos;

q) Los Estados Miembros deberían fomentar las alianzas público-privadas para combatir 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, los proveedores de servicios de comunicaciones y las instituciones académicas, con miras a aumentar los conocimientos y a mejorar la eficacia de las respuestas al delito cibernético;

r) Los Estados deberían adoptar medidas que alienten a los proveedores de servicios de Internet a desempeñar un papel en la prevención de la ciberdelincuencia y el apoyo a las actividades de aplicación de la ley y de investigación, por ejemplo estableciendo en su legislación nacional disposiciones pertinentes sobre las obligaciones de esos proveedores, así como definir claramente el alcance y los límites de esas obligaciones a fin de proteger los derechos e intereses legítimos de los proveedores de servicios;

s) Los Estados deberían reforzar las actividades de investigación y aplicación de la ley relacionadas con los actos de asociación, complicidad y preparación para cometer delitos cibernéticos, con miras a afrontar eficazmente toda la cadena de la ciberdelincuencia;

t) Los Estados deberían seguir reforzando la creación de capacidad y mejorando la capacidad de las autoridades judiciales y las fuerzas del orden para investigar y perseguir los delitos cibernéticos. En las actividades de creación de capacidad se debería hacer hincapié en los problemas cada vez mayores que plantean la computación en la nube, la web oscura y otras tecnologías emergentes. También se alienta a los Estados a que presten asistencia para el fomento de la capacidad a los países en desarrollo.

B. Pruebas electrónicas y justicia penal

11. 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 el marco del tema 3 del programa, titulado “Pruebas electrónicas y justicia penal”. 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:

a) Los Estados Miembros deberían establecer y aplicar facultades jurídicas, normas jurisdiccionales y otras disposiciones de procedimiento para permitir la investigación eficaz a nivel nacional del delito cibernético y los delitos facilitados por el uso de la tecnología, así como el logro de una cooperación efectiva en los casos transnacionales, teniendo en cuenta la necesidad de una aplicación eficaz de la ley, la soberanía nacional y la protección del derecho a la privacidad y otros derechos humanos. Ello puede incluir:

i) la adaptación de las normas probatorias para garantizar que las pruebas electrónicas puedan ser obtenidas, conservadas y autentificadas para su utilización en las actuaciones penales;

ii) la adopción de disposiciones sobre la localización nacional e internacional de las comunicaciones;

iii) la adopción de disposiciones relativas a la realización de registros electrónicos nacionales y transfronterizos;

iv) la adopción de disposiciones sobre la interceptación de comunicaciones transmitidas a través de redes de computadoras y medios similares;

v) la promulgación de leyes sustantivas y procesales que sean tecnológicamente neutras para que los países puedan hacer frente a las formas nuevas y emergentes de ciberdelincuencia;

vi) la armonización de la legislación nacional;

vii) la promulgación de nuevas leyes o el fortalecimiento de las existentes para permitir el reconocimiento de la admisibilidad de las pruebas electrónicas y definir y establecer el alcance de las pruebas electrónicas;

b) Los Estados Miembros deberían promover las iniciativas que fomenten la capacidad de los funcionarios encargados de hacer cumplir la ley, incluidos los que trabajan en estructuras especializadas de aplicación de la ley, los fiscales y la judicatura, de modo que posean al menos conocimientos técnicos básicos en materia de pruebas electrónicas y puedan reaccionar con eficacia y rapidez a las solicitudes de asistencia en la localización de comunicaciones, así como adoptar otras medidas necesarias para la investigación de delitos cibernéticos;

c) Los Estados Miembros deberían fomentar la creación de capacidad para mejorar las investigaciones, aumentar la comprensión de la ciberdelincuencia y del equipo y las tecnologías disponibles para combatirla, y permitir que los fiscales, jueces y autoridades nacionales centrales persigan esos delitos y resuelvan debidamente las causas relativas a ellos;

d) Los Estados Miembros deberían promover las iniciativas que fomenten la capacidad de las autoridades centrales que se ocupan de la cooperación internacional en materia de requisitos y procedimientos relativos a la asistencia judicial recíproca, entre otras cosas impartiendo capacitación sobre la redacción de solicitudes amplias con información suficiente para la obtención de pruebas electrónicas;

e) Los Estados Miembros deberían tener en cuenta el enfoque del “equipo de enjuiciamiento”, que combina los conocimientos y los recursos de diversos organismos y reúne a fiscales, agentes de investigación y analistas forenses para realizar investigaciones. Este enfoque permite a los fiscales manejar y presentar pruebas electrónicas;

f) La admisibilidad de las pruebas electrónicas no debería depender de si se han obtenido fuera de la jurisdicción de un país, siempre que no se les reste fiabilidad y que se obtengan lícitamente, por ejemplo, en virtud de un tratado de asistencia judicial recíproca o de un acuerdo multilateral, o en cooperación con el país que tenga jurisdicción;

g) Los Estados Miembros deberían adoptar las medidas necesarias para promulgar legislación que garantice la admisibilidad de las pruebas electrónicas, teniendo presente que la admisibilidad de pruebas, electrónicas o de otra índole, es una cuestión que cada país debería abordar de conformidad con su derecho interno;

h) Los Estados Miembros deberían intensificar la cooperación internacional entre los organismos encargados de hacer cumplir la ley, los fiscales, las autoridades judiciales y los proveedores de servicios de Internet a fin de salvar la distancia entre la rapidez con que operan los ciberdelincuentes y la agilidad de las respuestas de los organismos encargados de hacer cumplir la ley. Para ello, los Estados Miembros deberían valerse de los marcos existentes, como las redes de funcionamiento diario ininterrumpido y la cooperación por conducto de la Organización Internacional de Policía Criminal (INTERPOL), así como los tratados de asistencia judicial recíproca, a fin de fomentar la cooperación internacional en materia de pruebas electrónicas.

Los Estados Miembros deberían seguir armonizando y racionalizando los procesos relacionados con la asistencia judicial recíproca y elaborar un modelo común para agilizarlos con miras a la obtención y la transferencia oportunas de pruebas electrónicas transfronterizas;

i) Se alienta a los Estados Miembros a que aumenten el intercambio de experiencias e información, en particular sobre legislación nacional, procedimientos nacionales, mejores prácticas en materia de investigaciones transfronterizas sobre ciberdelincuencia, así como información sobre los grupos delictivos organizados y las técnicas y la metodología que utilizan;

j) Los Estados Miembros deberían establecer una red de coordinadores entre los organismos encargados de hacer cumplir la ley, las autoridades judiciales y los fiscales;

k) Los Estados Miembros deberían evaluar la posibilidad de encomendar al Grupo de Expertos o a los expertos de la UNODC que realicen, con la contribución de los Estados Miembros, una evaluación anual de las tendencias de la ciberdelincuencia y las nuevas amenazas, y que la pongan a disposición del público;

l) La UNODC debería apoyar la ampliación de las actividades de investigación para descubrir nuevas formas y modalidades de delincuencia, determinar los efectos de la delincuencia en esferas clave y conocer la evolución del entorno de las telecomunicaciones, incluida la expansión de la Internet de las cosas, la adopción de tecnologías de cadenas de bloques y criptomonedas y el uso de la inteligencia artificial junto con el aprendizaje automático;

m) Por conducto del Programa Mundial contra el Delito Cibernético, la UNODC debería promover, apoyar y poner en práctica, según proceda, proyectos de cooperación y asistencia técnica, con sujeción a la disponibilidad de recursos. En esos proyectos colaborarían expertos en prevención del delito, delitos contra la seguridad informática, legislación, enjuiciamiento, técnicas de investigación y cuestiones conexas con los Estados que desearan solicitar información o asistencia en esas esferas;

n) La UNODC debería establecer un programa educativo centrado en aumentar los conocimientos y la sensibilización de las autoridades judiciales y el ministerio público de los Estados Miembros sobre las medidas de lucha contra la ciberdelincuencia, especialmente en la esfera de la obtención de pruebas electrónicas;

o) Los Estados Miembros deberían adoptar medidas encaminadas a aumentar la cooperación en la obtención de pruebas electrónicas, entre las que cabría mencionar:

i) el intercambio de información sobre las amenazas de la ciberdelincuencia;

ii) el intercambio de información sobre los grupos de ciberdelincuencia organizada, en particular las técnicas y la metodología que utilizan;

iii) la promoción de una mayor cooperación y coordinación entre los organismos encargados de hacer cumplir la ley, los fiscales y las autoridades judiciales;

iv) el intercambio de estrategias e iniciativas nacionales para hacer frente a la ciberdelincuencia, incluso en materia de legislación y procedimientos nacionales para llevar a los ciberdelincuentes ante la justicia;

v) el intercambio de las mejores prácticas y experiencias relacionadas con la investigación transfronteriza de la ciberdelincuencia;

vi) el establecimiento de una red de puntos de contacto entre los organismos encargados de hacer cumplir la ley, las autoridades judiciales y los fiscales;

vii) la armonización y racionalización de los procesos relacionados con la asistencia judicial recíproca y la elaboración de un modelo común para agilizar el proceso con miras a la obtención y la transferencia oportunas de pruebas electrónicas transfronterizas;

viii) la impartición de cursos prácticos y seminarios para reforzar la capacidad de las autoridades encargadas de hacer cumplir la ley y las autoridades judiciales de redactar solicitudes, en el contexto de los tratados de asistencia judicial recíproca, a fin de obtener pruebas en cuestiones relacionadas con la ciberdelincuencia;

ix) la elaboración de normas y el aumento de la uniformidad en los aspectos procesales relativos a la obtención y la transferencia de pruebas digitales;

x) la formulación de un enfoque común respecto de los acuerdos de intercambio de información con los proveedores de servicios en relación con la investigación de delitos cibernéticos y la obtención de pruebas;

xi) la interacción con los proveedores de servicios mediante alianzas público-privadas a fin de establecer modalidades de cooperación en la aplicación de la ley, la investigación de delitos cibernéticos y la obtención de pruebas;

xii) la elaboración de directrices para que los proveedores de servicios presten asistencia a los organismos encargados de hacer cumplir la ley en las investigaciones de delitos electrónicos, en particular respecto del formato y la duración de la conservación de las pruebas y la información digitales;

xiii) el fortalecimiento de la capacidad técnica y jurídica de los organismos encargados de hacer cumplir la ley, los jueces y los fiscales mediante programas de creación de capacidad y desarrollo de aptitudes;

xiv) la prestación de asistencia a los países en desarrollo para fortalecer la capacidad forense en el ámbito cibernético, incluso mediante el establecimiento de laboratorios de ciencias forenses especializados en esa materia;

xv) la impartición de talleres y seminarios para dar a conocer las mejores prácticas en la lucha contra la ciberdelincuencia;

xvi) el establecimiento de un organismo internacional que valide y certifique instrumentos digitales para estudios forenses, además de la preparación de manuales y el fortalecimiento de la capacidad de las fuerzas del orden y de las respuestas judiciales a la ciberdelincuencia;

p) Los países deberían invertir en la creación y mejora de la capacidad forense digital, sobre todo en materia de capacitación y certificados de seguridad, así como en sistemas de gestión de la seguridad de la información para contribuir al éxito de los procesos judiciales por delitos cibernéticos mediante el examen de dispositivos electrónicos con el fin de asegurar la fiabilidad de las pruebas que se obtengan;

q) En los sistemas jurídicos que utilizan el modelo inquisitivo, en que los funcionarios judiciales son también investigadores, la judicatura debería recibir capacitación especializada en materia de ciberdelincuencia;

r) Dado que algunos jueces no están familiarizados con las pruebas digitales, este tipo de pruebas suele estar sujeta a normas más estrictas en lo que respecta a su autentificación y admisión. Sin embargo, debe tenerse en cuenta que no hay ninguna razón práctica para imponer normas más estrictas en relación con la integridad de las pruebas digitales a diferencia de las pruebas tradicionales. Las probabilidades de que las pruebas digitales se hayan modificado o inventado no son mayores que las de otros tipos de pruebas. De hecho, podría decirse que es más difícil modificar o inventar pruebas digitales porque se pueden utilizar varios algoritmos matemáticos, como los valores segmentados (valores “hash”), como método de autentificación o para indicar una modificación;

s) Los Estados deberían aumentar la eficacia de la coordinación y las sinergias interinstitucionales nacionales, incluido el intercambio de información e inteligencia fiables, con el sector privado, las organizaciones de la sociedad civil y otros interesados para contribuir a la eficacia de la cooperación y la colaboración internacionales;

t) Los Estados deberían promulgar nuevas leyes o fortalecer las existentes de modo que sea posible reconocer la admisibilidad de las pruebas electrónicas, así como definir y establecer su alcance;

u) Sería conveniente que los Estados consideraran la posibilidad de establecer en su legislación interna que los datos siguientes pueden constituir pruebas electrónicas: los datos de tráfico, como los ficheros de registro; los datos de contenido, como los correos electrónicos; los datos de los abonados, como la información de registro de los usuarios; y otros datos que se almacenan, procesan y transmiten en formato digital y que se generan durante la comisión de un delito y, por lo tanto, pueden utilizarse para establecer los hechos de ese delito;

v) Se alienta a los Estados a que refuercen la creación de capacidad para la obtención de pruebas electrónicas, creen equipos profesionales dotados de conocimientos jurídicos y técnicos y mejoren el intercambio de experiencias y la cooperación en materia de capacitación a ese respecto. Se alienta a la UNODC a que desempeñe un papel en esos esfuerzos;

w) Se alienta a los Estados a que establezcan en su legislación interna métodos pertinentes para la obtención de pruebas electrónicas, como la incautación y conservación del medio de almacenamiento original, la obtención *in situ*, la obtención a distancia y la verificación. Se alienta a los Estados Miembros a que sometan a embargo las pruebas electrónicas para evitar su supresión o modificación, o la adición de otros elementos, mediante medidas como el cómputo de la suma de verificación de las pruebas electrónicas, el bloqueo de las cuentas de aplicaciones web y la adopción de medidas de protección contra escritura;

x) Se alienta a los Estados a que establezcan normas y estándares técnicos respecto de la obtención de pruebas electrónicas;

y) Los Estados deberían velar por que la obtención de pruebas electrónicas se ajuste a las normas del debido proceso;

z) Los Estados deberían establecer normas para evaluar la autenticidad, integridad, legalidad y pertinencia de las pruebas electrónicas en su legislación nacional y tener en cuenta las características singulares de ese tipo de pruebas al aplicar las normas sobre pruebas originales, testimonios de oídas y exclusión de pruebas ilegales;

aa) Al obtener pruebas electrónicas en el extranjero, se debería respetar la soberanía de los Estados donde se encuentran los datos, ajustarse a las normas del debido proceso y respetar los derechos legítimos de las personas y entidades pertinentes. Los Estados también deberían abstenerse de utilizar unilateralmente medidas de investigación técnica intrusivas o destructivas a este respecto;

bb) Se alienta a los Estados a que celebren consultas con otros Estados a fin de seguir mejorando la asistencia judicial internacional y la cooperación en materia de aplicación de la ley mediante la optimización de los procedimientos y métodos pertinentes, a fin de facilitar la investigación de la ciberdelincuencia y la obtención de pruebas electrónicas;

cc) Los Estados deberían considerar la posibilidad de adoptar disposiciones internacionales modelo sobre las facultades de investigación relativas a la obtención de pruebas electrónicas, así como de negociar, en el marco de las Naciones Unidas, un instrumento mundial vinculante para combatir la ciberdelincuencia. Ese instrumento puede incluir disposiciones universalmente aceptadas sobre la obtención transfronteriza de pruebas electrónicas.

III. Resumen de las deliberaciones

A. Aplicación de la ley e investigaciones

12. En sus sesiones primera, segunda y tercera, celebradas los días 27 y 28 de marzo de 2019, el Grupo de Expertos examinó el tema 2 del programa, titulado “Aplicación de la ley e investigaciones”.

13. Facilitaron el debate los siguientes panelistas: Shenkuo Wu (China); Ioana Albani (Rumania); Martín Gershanik (Argentina); Pedro Verdelho (Portugal); y Anton Kurdyukov (Federación de Rusia).

14. En el debate posterior, el Grupo de Expertos examinó algunos ejemplos de supuestas actividades delictivas llevadas a cabo 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. Asimismo, se informó al Grupo de Expertos sobre la interdependencia conceptual entre la ciberdelincuencia y la ciberseguridad, así como sobre las distinciones entre ambas, además de 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 de criptomonedas y su extracción con fines maliciosos; y la clonación de tarjetas y delitos conexos.

15. Se debatió una vez más si era necesario un instrumento jurídico global y exhaustivo sobre la ciberdelincuencia o si los Estados deberían centrarse en la aplicación efectiva de los instrumentos existentes, en particular el Convenio de Budapest. Algunos oradores sostuvieron que no se necesitaban más instrumentos jurídicos sobre ciberdelincuencia, dado que el Convenio de Budapest ofrecía un marco adecuado para elaborar respuestas adecuadas contra el delito cibernético a nivel nacional e internacional. Se observó que 63 Estados partes se habían adherido al Convenio de Budapest, lo que demostraba que estaba abierto a la adhesión de Estados que no fueran miembros del Consejo de Europa. Además, se destacó que algunos Estados que no eran partes en el Convenio lo utilizaban como fuente de inspiración para armonizar las normas legislativas nacionales de carácter sustantivo y procesal. También se señaló que el concepto 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, aprobada en 2014, y el Código Internacional de Conducta para la Seguridad de la Información, publicado por la Organización de Cooperación de Shanghái.

16. No obstante, otros oradores sostuvieron que era necesario adoptar un 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, además, no todos los Estados del mundo eran partes. Se destacó que ese instrumento se elaboraría como parte 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 a la resolución 73/187 de la Asamblea General, de 17 de diciembre de 2018, relativa a 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. También se expresó la opinión de que el Convenio de Budapest no era lo suficientemente transparente o inclusivo, no abordaba las preocupaciones de todos los Estados Miembros y establecía procesos complejos y poco transparentes para modificar su texto, lo que podría ser una desventaja en vista de la naturaleza en constante evolución de la ciberdelincuencia.

17. 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 algunas de las siguientes cuestiones, o con todas ellas: 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; y un marco y unas salvaguardias estrictas respecto de las prácticas que impliquen el acceso transfronterizo a los datos, que incluyan requisitos de protección de datos.

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

19. 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 aplicar medidas jurídicas y de procedimiento destinadas a combatir el delito cibernético. Según varios oradores, 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 la reforma legislativa a nivel nacional, incluido el alcance de dicha reforma. Se puso de relieve la necesidad de contar con procesos inclusivos y participativos para que se tuvieran en cuenta 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*, y a la necesidad de utilizar un lenguaje “tecnológicamente neutro” en la nueva legislación, de modo que esta siguiera siendo compatible con los rápidos avances en el ámbito de las tecnologías de la información y las comunicaciones.

20. Las deliberaciones también giraron en torno a los problemas que planteaban los conflictos relacionados con la jurisdicción territorial, 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 destacó que sería útil adoptar enfoques flexibles sobre la cuestión de las bases jurisdiccionales aplicables en el ámbito de la ciberdelincuencia, por ejemplo, concediendo más importancia al lugar desde el que se prestaran los servicios de tecnologías de la información y de las comunicaciones que a la ubicación de los datos.

21. El Grupo de Expertos subrayó además la necesidad de contar con facultades procesales adecuadas para obtener pruebas electrónicas, por ejemplo, datos y metadatos para las investigaciones relacionadas no solo con el delito cibernético sino también con otras formas de delincuencia. Esas pruebas electrónicas podían consistir en información sobre los abonados, datos de contenido o datos de tráfico. Se señaló 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, y que 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. Se concedió prioridad al fortalecimiento de la función de coordinación de las autoridades nacionales competentes, como los fiscales generales o las fiscalías especializadas.

22. 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. 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 Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos sobre el derecho a la privacidad en la era digital (A/HRC/27/37), presentado ante el Consejo de Derechos Humanos de conformidad con la resolución 68/167 de la Asamblea General.

23. El Grupo de Expertos reiteró la importancia de la cooperación internacional en la investigación transfronteriza y persecución de los delitos cibernéticos. Varios oradores observaron que el número de solicitudes de asistencia judicial recíproca para obtener y conservar pruebas electrónicas iba en rápido aumento y que las modalidades tradicionales de cooperación, especialmente las que algunos consideraban procesos prolongados relativos a la asistencia judicial recíproca, no facilitaban el rápido acceso a los datos. Otros observaron que la asistencia judicial recíproca seguía siendo un instrumento fundamental para el intercambio transfronterizo de datos. Algunos oradores también señalaron que la creación de capacidad y la capacitación sobre las necesidades relacionadas con la asistencia judicial recíproca, incluida la redacción de solicitudes amplias con información suficiente para obtener pruebas electrónicas, eran componentes clave para asegurar la transmisión oportuna de los datos. Además, algunos países recomendaron el uso de redes de funcionamiento diario ininterrumpido para solicitar la pronta conservación de los datos debido a la naturaleza volátil de ese tipo de pruebas, que podrían transferirse o suprimirse con un simple clic del ratón.

24. Se mencionaron distintos ejemplos de prácticas que contribuirían a promover la cooperación internacional en lo que concierne a las pruebas electrónicas, particularmente a nivel operacional. Entre esas prácticas figuraba la transmisión directa de 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; 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; 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, creado en 2013 por la Agencia de la Unión Europea para la Cooperación Policial con el fin de fortalecer las respuestas de las autoridades encargadas de la aplicación de la ley ante la ciberdelincuencia dentro de la Unión Europea.

25. El Grupo de Expertos también trató la cuestión del acceso transfronterizo a los datos. En general, se observó que las prácticas y procedimientos utilizados por los Estados y las condiciones y salvaguardias relacionadas con ellos variaban considerablemente. Se expresó preocupación por los posibles problemas jurídicos causados por determinadas prácticas en relación con el acceso transfronterizo a los datos. Además, se hizo hincapié en los derechos procesales de los sospechosos, las consideraciones relativas a la privacidad y la protección de los datos personales, los

métodos de acceso a los datos almacenados en otra jurisdicción y la legalidad de dicho acceso, así como el respeto al principio de la soberanía nacional.

26. El Grupo de Expertos recalcó la importancia de la creación sostenible de capacidad para mejorar la eficacia y las cualificaciones de todos los actores 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 distintos Estados. Algunos oradores se refirieron también a la mejora de la capacitación y la creación de capacidad, sumadas al establecimiento de estructuras o unidades especializadas en ciberdelincuencia en el ministerio público y las fuerzas del orden. A ese respecto, se subrayó que, dado que las pruebas electrónicas eran cada vez más comunes en la investigación de otras formas de delincuencia, era esencial establecer estructuras especializadas que ofrecieran conocimientos especializados, experiencia y aptitudes operacionales para la investigación de esos delitos.

27. El Grupo de Expertos examinó además la importancia de fomentar y fortalecer la cooperación entre las autoridades nacionales y el sector privado, en particular los proveedores de servicios de comunicaciones y los proveedores de servicios de Internet, a fin de mejorar la conservación de los datos y el acceso a ellos. 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 hizo referencia al riesgo de que los proveedores de servicios de comunicaciones y los proveedores de servicios de Internet tuvieran que hacer frente a requisitos contradictorios, es decir, cómo equilibrar sus respuestas teniendo en cuenta los requisitos jurídicos de los Estados implicados.

28. 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; aplicar nuevos instrumentos de investigación para obtener pruebas electrónicas y determinar su autenticidad a efectos probatorios en actuaciones penales, teniendo en cuenta las salvaguardias de los derechos humanos; poner en práctica acuerdos institucionales orientados a hacer un uso más eficiente de los recursos en la lucha contra la ciberdelincuencia; y promover la cooperación internacional contra la ciberdelincuencia. Un orador dijo que las diferencias entre la ciberseguridad y la ciberdelincuencia eran la consideración más importante al estructurar las respuestas nacionales y definir las competencias institucionales en la materia.

29. 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 los intercambios 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. También se mencionó el valor que añadía de la Comisión a ese respecto. Se afirmó que el Grupo de Expertos tenía el mandato especial de servir de plataforma para los debates sobre el tema, aunque ello no excluiría necesariamente otras iniciativas encaminadas a desarrollar una gobernanza mundial amplia para combatir la ciberdelincuencia.

30. Se expresó apoyo a la labor realizada por la UNODC en los ámbitos de la asistencia técnica y la creación de capacidad para establecer respuestas bien cohesionadas a la ciberdelincuencia.

31. 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 fue redactada y presentada conjuntamente por la UNODC, la Dirección Ejecutiva del Comité contra el Terrorismo y la Asociación Internacional de Fiscales y se había puesto a disposición de los Estados Miembros y sus funcionarios de justicia penal a través del portal SHERLOC de la UNODC. La Guía, elaborada en colaboración con los Estados Miembros, otras

organizaciones internacionales y regionales, y proveedores de servicios de comunicaciones como Facebook, Google, Microsoft y Uber, contenía información sobre medidas que se podrían adoptar a nivel nacional para reunir, conservar y compartir pruebas electrónicas con el objetivo general de asegurar la eficiencia en la práctica de la asistencia judicial recíproca.

B. Pruebas electrónicas y justicia penal

32. En sus sesiones cuarta y quinta, celebradas los días 28 y 29 de marzo de 2019, el Grupo de Expertos examinó el tema 3 del programa, titulado “Pruebas electrónicas y justicia penal”.

33. Facilitaron el debate los siguientes panelistas: Xioafei Zhai (China); Markko Kunnapu (Estonia); Camila Bosch (Chile); Giuseppe Corasaniti (Italia); Vadim Smekhnov (Federación de Rusia); y Briony Daley Whitworth (Australia).

34. En el debate subsiguiente, se destacó el hecho de que las pruebas electrónicas cumplían una doble función. Por una parte, se reconoció que el uso de la tecnología e infraestructura digital creaba más oportunidades para que los autores de delitos graves y organizados facilitados por la cibernética incrementaran sus actividades ilícitas, accedieran a un mayor número de víctimas y aumentaran sus ganancias. Por otra parte, también se subrayó que las pruebas electrónicas estaban adquiriendo cada vez mayor importancia en la detección, la investigación y la persecución de todos los tipos de delitos.

35. Muchos oradores se refirieron a la creciente importancia de las pruebas electrónicas en las actuaciones penales y describieron los diversos enfoques nacionales para definir el alcance de esas pruebas. Algunos observaron que no existía a nivel internacional una definición común de pruebas electrónicas, mientras que la formulación de normas en la materia y la admisibilidad de las pruebas a nivel nacional era prerrogativa de los Estados Miembros. Señalaron la necesidad de una legislación procesal que otorgara a las autoridades competentes encargadas de hacer cumplir la ley la facultad de obtener pruebas electrónicas de manera eficaz, respetando al mismo tiempo la confidencialidad, la privacidad, los derechos humanos, las normas del debido proceso y otras salvaguardias jurídicas. Se destacó que las facultades de investigación podían ser desde facultades procesales tradicionales y facultades generales de investigación hasta diversas técnicas concretas de investigación digital.

36. Se convino en que una de las medidas clave en las investigaciones sobre la ciberdelincuencia y las investigaciones digitales consistía en preservar la integridad de las pruebas electrónicas y garantizar su autenticidad y su admisibilidad en las actuaciones penales conexas. En ese contexto, se hizo referencia a las normas, procedimientos y requisitos nacionales relativos al manejo de pruebas electrónicas. El Grupo de Expertos destacó una vez más la necesidad de fomentar la capacidad y los conocimientos técnicos de las autoridades competentes para que hicieran frente con eficacia y eficiencia a los retos que se plantean.

37. El Grupo de Expertos examinó los factores que se consideraban pertinentes al determinar la admisibilidad de las pruebas electrónicas. Se hizo hincapié en la importancia de cumplir el principio de proporcionalidad al utilizar técnicas especiales en las investigaciones de delitos cibernéticos, incluida la utilización de agentes encubiertos y técnicas forenses remotas, especialmente en la web oscura. Se observó que en muchos ordenamientos jurídicos nacionales ese principio era puesto a prueba principalmente por la autoridad judicial que supervisaba la investigación y por el tribunal, según procediera. La pertinencia puede determinarse en función de la gravedad del delito de que se trate o del número de personas cuyo derecho a la privacidad haya sido violado por las técnicas especiales de investigación utilizadas, los tipos de datos informáticos de que se trate, si es posible aplicar alguna medida menos restrictiva, si ha habido algún grado de imparcialidad en el proceso de adopción de decisiones y si las personas afectadas han tenido oportunidades adecuadas para obtener reparación legal.

38. Se hizo hincapié en que cada vez más programas y aplicaciones incorporaban métodos de cifrado, lo que hacía que el acceso a datos que sirvieran como pruebas electrónicas entrañara un proceso difícil y dilatado si no se contaba con las claves de descifrado adecuadas. Se formularon sugerencias prácticas sobre la manera de superar ese problema, por ejemplo, mediante la cooperación con otros países que tengan la capacidad de acceder a información cifrada, la utilización del Centro Europeo contra la Delincuencia Informática y la cooperación con la industria, que podría desarrollar mecanismos que permitieran un acceso oportuno a los datos cifrados.

39. También se mencionó el uso de la inteligencia artificial en las investigaciones, haciendo especial referencia al reconocimiento facial y a las violaciones de los derechos de autor. En general, la inteligencia artificial podría aportar soluciones que permitan un mejor aprovechamiento del tiempo y los recursos cuando se examinaran grandes volúmenes de datos en busca de pruebas electrónicas importantes.

40. Se indicó que la información sobre los abonados era el tipo de datos que las autoridades de la justicia penal solicitaban con más frecuencia en las investigaciones penales de delitos cibernéticos y otros casos relacionados con pruebas electrónicas. A ese respecto, muchos oradores se refirieron a las dificultades asociadas con la información sobre los abonados que utilizaban una dirección de Protocolo de Internet (IP) específica que se detectara en la comisión de un delito. Se observó que, si bien las direcciones IP estáticas eran estables y se asignaban a un abonado específico mientras estuviera vigente el acuerdo de servicios, y aunque los proveedores podían encontrar esa información en las bases de datos de abonados, también era posible que se asignara una misma dirección IP a varios usuarios. Por lo tanto, era necesario determinar a qué abonado se había asignado la dirección IP en un momento determinado. También se señaló que las direcciones IP se asignaban de forma dinámica porque en la versión 4 del Protocolo de Internet había un número limitado de direcciones. Ese problema se resolvería una vez que la transición a la versión 6 del Protocolo de Internet se hubiera finalizado o se encontrara en una fase más avanzada.

41. También se examinó la cuestión de la diferenciación entre los tipos de datos solicitados y sus consecuencias desde el punto de vista de la eficacia y la puntualidad de los mecanismos de cooperación internacional para obtener pruebas electrónicas. Las soluciones examinadas se referían, entre otras cosas, al fortalecimiento de la cooperación en la aplicación de la ley, la reanudación del diálogo multilateral sobre el acceso transnacional a los datos informáticos y el establecimiento de un régimen aparte para el acceso a la información sobre los abonados, según se define en el artículo 18, párrafo 3, del Convenio de Budapest.

42. Muchos oradores se refirieron a los problemas que planteaban las criptomonedas en las investigaciones de delitos cibernéticos. Se informó al Grupo de Expertos acerca del curso de formación de formadores sobre investigación de criptomonedas, impartido por la UNODC. Su objetivo era reforzar la capacidad de los funcionarios encargados de hacer cumplir la ley, los analistas, los fiscales y los jueces en relación con las criptomonedas, en particular cómo localizar bitcoines en una investigación financiera, hallar recursos de información y colaborar en materia de tramitación de casos en el plano internacional.

43. En relación con el tema 3 del programa, algunos oradores abordaron cuestiones jurisdiccionales. Se hizo especial referencia a la evolución reciente de la jurisprudencia nacional respecto de la interpretación del principio de territorialidad en los casos en que los datos informáticos se encontraran en servidores en la nube en otras jurisdicciones.

44. Los oradores coincidieron en que la cooperación internacional era de suma importancia para la obtención y el intercambio de pruebas electrónicas en el contexto de las investigaciones transfronterizas. Se subrayó que los Estados deberían aplicar plenamente la Convención contra la Delincuencia Organizada y los tratados y acuerdos multilaterales, regionales y bilaterales pertinentes sobre ciberdelincuencia para fomentar la cooperación internacional en materia de asistencia judicial y aplicación de la ley en casos conexos, respetando al mismo tiempo los principios de soberanía, igualdad y reciprocidad. Se destacó la importancia de promover la creación de redes

para el intercambio de experiencias y conocimientos especializados, en particular para hacer frente a los problemas derivados de la disparidad de requisitos nacionales en materia de admisibilidad, y de integridad y autenticidad de ese tipo de pruebas.

45. Muchos oradores consideraron prioritaria la necesidad de que se fomentara la capacidad sostenible en los organismos nacionales encargados de hacer cumplir la ley y los sistemas de justicia penal, incluido el fomento de la capacidad de los profesionales de las autoridades centrales que se ocupan de la cooperación internacional. Se señaló que esas actividades de creación de capacidad eran esenciales, en particular para los países en desarrollo, desde el punto de vista de los recursos humanos, la infraestructura y el equipo, y con miras a superar la brecha digital que los separa de los países desarrollados. En general, se convino en que el desarrollo de la capacidad de los encargados de hacer cumplir la ley y de la justicia penal frente a la ciberdelincuencia sería un proceso continuo, puesto que las innovaciones técnicas y delictivas seguían avanzando a un ritmo acelerado. Así pues, la gran mayoría de los oradores se refirieron a la asistencia técnica y la cooperación como requisitos primordiales para mejorar la capacidad nacional y permitir el intercambio de buenas prácticas y experiencias en materia de investigación, así como la difusión de nuevas técnicas.

46. A ese respecto, varios oradores se refirieron a las dificultades que planteaban los limitados recursos en la esfera de las ciencias forenses, la falta de instrumentos y equipo para estudios forenses, cuyo costo a menudo era elevado, y el enorme volumen de datos que se obtenía para su análisis. También se informó de las dificultades para contratar a personal suficientemente cualificado.

C. Otros asuntos

47. En su sexta sesión, celebrada el 29 de marzo de 2019, el Grupo de Expertos examinó el tema 4 del programa, titulado “Otros asuntos”.

48. Un orador pidió información acerca del informe sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones, que se presentaría a la Asamblea General en su septuagésimo cuarto período de sesiones, de conformidad con la resolución 73/187 de la Asamblea. En respuesta, un representante de la Secretaría se refirió al mandato que figuraba en la resolución y destacó que el 13 de febrero de 2019 se había enviado una nota verbal a los Estados Miembros en la que se les invitaba a presentar información sobre los problemas a que se enfrentaban para combatir la utilización de las tecnologías de la información y las comunicaciones con fines delictivos y se les indicaba que esa información se utilizaría para preparar el informe. Se fijó el viernes 12 de abril de 2019 como fecha límite para presentar los comentarios nacionales. Al vencerse ese plazo, la Secretaría recopilaría los comentarios recibidos con miras a ultimar el informe en mayo de 2019.

IV. Organización de la reunión

A. Apertura de la reunión

49. Declaró abierta la reunión André Rypl (Brasil), Vicepresidente del Grupo de Expertos, en su calidad de Presidente de la quinta reunión del Grupo de Expertos.

B. Declaraciones

50. Formularon declaraciones expertos de los siguientes Estados Miembros: Alemania, Argelia, Argentina, Armenia, Australia, Belarús, Brasil, Burkina Faso, Canadá, Chile, China, Colombia, Costa Rica, Ecuador, Emiratos Árabes Unidos, Eslovaquia, España, Estados Unidos de América, Estonia, Federación de Rusia, Filipinas, Francia, Georgia, India, Indonesia, Irán (República Islámica del), Italia, Japón, Jordania, Kuwait, Malasia, Mauritania, México, Marruecos, Níger, Nigeria,

Noruega, Países Bajos, Paraguay, Perú, República Dominicana, Reino Unido de Gran Bretaña e Irlanda del Norte, Serbia, Sri Lanka, Sudáfrica, Tailandia y Viet Nam.

51. Formularon declaraciones también los representantes de dos organizaciones intergubernamentales: Consejo de Europa y Unión Europea.

C. Aprobación del programa y otras cuestiones de organización

52. En su primera sesión, celebrada el 27 de marzo de 2019, el Grupo de Expertos aprobó el siguiente programa provisional:

1. Cuestiones de organización:
   a) apertura de la reunión;
   b) aprobación del programa.
2. Aplicación de la ley e investigaciones.
3. Pruebas electrónicas y justicia penal.
4. Otros asuntos.
5. Aprobación del informe.

D. Asistencia

53. Asistieron a la reunión representantes de 105 Estados Miembros, un instituto de la red del programa de las Naciones Unidas en materia de prevención del delito y justicia penal, organizaciones intergubernamentales y el sector privado.

54. En el documento UNODC/CCPCJ/EG.4/2019/INF/1/Rev.1 figura la lista de participantes.

E. Documentación

55. 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 anotado (UNODC/CCPCJ/EG.4/2019/1);

b) programa 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

56. En su sexta sesión, celebrada el 29 de marzo de 2019, el Grupo de Expertos aprobó su informe (UNODC/CCPCJ/EG.4/2019/2).