19 de abril de 2021
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 6 al 8 de abril de 2021

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 ocasión el Grupo de Expertos examinó y aprobó un conjunto de temas y una metodología para la realización del 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 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, proyecto este 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.

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 en 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 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 en Viena del 10 al 13 de abril de 2017. En esa reunión el Grupo de Expertos examinó, entre otros aspectos, la posibilidad de aprobar los resúmenes del Relator sobre las deliberaciones de las reuniones 1ª y 2ª, 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 a nivel nacional e internacional frente al delito cibernético.

7. La cuarta reunión del Grupo de Expertos se celebró en Viena del 3 al 5 de abril de 2018. En esa ocasión la labor se centró en la legislación y los marcos relativos al delito cibernético y en la tipificación de ese delito. También se examinaron las novedades legislativas y de políticas registradas en los planos nacional e internacional en lo que respecta a la lucha contra el delito cibernético. Además, el Grupo de Expertos estudió diversas modalidades utilizadas por los países para tipificar la ciberdelincuencia. Asimismo, en esa reunión se aprobó la propuesta de plan de trabajo del Grupo de Expertos para el período 2018-2021 presentada por la Presidencia (UNODC/CCPCJ/EG.4/2018/CRP.1).

8. La quinta reunión del Grupo de Expertos se celebró en Viena del 27 al 29 de marzo de 2019. En esa reunión el Grupo de Expertos se centró en la aplicación de la ley y las investigaciones, así como en las pruebas electrónicas y la justicia penal en relación con el delito cibernético. Se proporcionó información, por ejemplo, acerca de las iniciativas que se habían puesto en marcha con éxito a nivel de los países para aplicar leyes y procedimientos destinados a combatir el delito cibernético y nuevos instrumentos de investigación encaminados a obtener pruebas electrónicas y determinar su autenticidad a efectos probatorios en actuaciones penales. Las deliberaciones se centraron, además, en la manera de conciliar la necesidad de que los organismos encargados de hacer cumplir la ley articulen respuestas eficaces frente a la ciberdelincuencia con la protección de los derechos humanos fundamentales, en especial el derecho a la privacidad. El Grupo de Expertos consideró prioritario satisfacer la necesidad de fomentar la capacidad de manera sostenible con objeto de reforzar la capacidad de los países y favorecer el intercambio de buenas prácticas y experiencias de investigación.

9. En la sexta reunión del Grupo de Expertos, celebrada en Viena del 27 al 29 de julio de 2020, el Relator elaboró una lista de recomendaciones y conclusiones preliminares en materia de cooperación internacional y prevención. Conforme al plan de trabajo del Grupo de Expertos para el período 2019-2021, esa lista se incluyó en el informe de la sexta reunión (UNODC/CCPCJ/EG.4/2020/2), en forma de recopilación de las sugerencias formuladas por los Estados Miembros, a efectos de someterla a examen posteriormente, en la reunión de evaluación que se celebraría a más tardar en 2021.

10. El 23 de noviembre de 2020 la Mesa ampliada del Grupo de Expertos, mediante el procedimiento de acuerdo tácito, aprobó las fechas del 6 al 8 de abril de 2021 para la celebración de la séptima reunión del Grupo de Expertos. El 14 de diciembre de 2020 también aprobó por acuerdo tácito el programa provisional de la séptima reunión. Además, el 11 de marzo de 2021 se decidió por acuerdo tácito que la reunión se celebrara en formato híbrido/con presencia de la Presidencia, habida cuenta de que persistía la situación creada por la enfermedad por coronavirus (COVID-19). En la reunión de la

Mesa ampliada celebrada el 31 de marzo de 2021 se convino en que únicamente se presentara un informe de procedimiento de la séptima reunión, que no contuviera un resumen de las deliberaciones elaborado por el Presidente, pero sí un anexo en el que figuraran las conclusiones y recomendaciones.

II. Organización de la reunión

A. Apertura de la reunión

11. Declaró abierta la reunión André Rypl (Brasil), Vicepresidente del Grupo de Expertos, en calidad de Presidente de la séptima reunión del Grupo de Expertos.

B. Aprobación del programa y otras cuestiones de organización

12. En su primera sesión, celebrada el 6 de abril de 2021, el Grupo de Expertos aprobó el siguiente programa provisional:

1. Cuestiones de organización:
   a) Apertura de la reunión;
   b) Aprobación del programa.
2. Examen de las conclusiones y recomendaciones preliminares resultantes de las reuniones 4ª, 5ª y 6ª del Grupo de Expertos, celebradas en 2018, 2019 y 2020, y elaboración de conclusiones y recomendaciones para presentarlas a la Comisión de Prevención del Delito y Justicia Penal.
3. Examen de la labor futura del Grupo de Expertos.
4. Otros asuntos.
5. Aprobación del informe.

C. Declaraciones

13. En relación con el tema 1 del programa, y a propuesta del Presidente, el Grupo de Expertos acordó que las delegaciones se abstendrían de hacer declaraciones de carácter general. También se acordó que, en relación con los temas 2 y 3 del programa, debido a las restricciones de tiempo, las declaraciones se limitarían a un máximo de 3 minutos, y que las delegaciones tendrían, además, la posibilidad de enviar sus declaraciones por escrito a la Secretaría, que las publicaría en el sitio web de la séptima reunión del Grupo de Expertos.

14. En relación con el tema 3 del programa formularon declaraciones los delegados de Australia, Chile, Colombia, la Unión Europea (en nombre de sus Estados miembros), el Yemen, la República Dominicana, el Brasil, los Países Bajos, la República Bolivariana de Venezuela, Nueva Zelandia, Guatemala, Nigeria, los Estados Unidos de América, China, la Federación de Rusia, Francia, Cuba, el Japón, Sudáfrica, Polonia, el Canadá, Bélgica, Austria, la Argentina, Noruega, la República Islámica del Irán, Portugal, Kirguistán, Honduras, el Reino Unido de Gran Bretaña e Irlanda del Norte, la India, México, Nicaragua y la República Árabe Siria.

D. Organización de los trabajos

15. En su primera sesión, celebrada el 6 de abril, el Grupo de Expertos comenzó a examinar la lista de conclusiones y recomendaciones relativas a la legislación y los marcos y a la tipificación de delitos, que figuran en el documento de sesión titulado “Recopilación de todas las conclusiones y recomendaciones preliminares sugeridas por los Estados Miembros durante las reuniones del Grupo de Expertos encargado de

realizar un estudio exhaustivo sobre el delito cibernético celebradas en 2018, 2019 y 2020” (UNODC/CCPCJ/EG.4/2021/CRP.1). Para ello, el Presidente invitó a las delegaciones a que indicaran si tenían objeciones a las conclusiones y recomendaciones, ya fueran de fondo o de redacción, y las objeciones se incluyeron en un documento evolutivo que se proyectó en pantalla y posteriormente se puso a disposición de las delegaciones por vía electrónica.

16. En su segunda sesión, también celebrada el 6 de abril, el Grupo de Expertos terminó la primera lectura de la lista de conclusiones y recomendaciones preliminares correspondientes a sus reuniones de 2018 y 2019, y comenzó a examinar a fondo aquellas sobre las que no se había logrado consenso por problemas de redacción.

17. En su tercera sesión, celebrada el 7 de abril, el Grupo de Expertos finalizó la primera lectura de la lista de conclusiones y recomendaciones preliminares correspondientes a su reunión de 2020 y siguió examinando en detalle algunas de aquellas respecto de las cuales no se había llegado a un consenso. También examinó el modo de señalar a la atención de la Comisión esas conclusiones y recomendaciones.

18. En su cuarta sesión, celebrada el 7 de abril, el Grupo de Expertos siguió examinando en detalle algunas conclusiones y recomendaciones sobre las que no se había logrado consenso. Se expresaron opiniones divergentes respecto de presentarlas o no a la Comisión.

19. En su quinta sesión, celebrada el 8 de abril, el Grupo de Expertos siguió examinando la conveniencia de presentar o no a la Comisión las conclusiones y recomendaciones preliminares sobre las que no había consenso. El Presidente propuso que en el presente informe quedara reflejado el hecho de que el Grupo de Expertos había examinado todas las conclusiones y recomendaciones contenidas en el documento UNODC/CCPCJ/EG.4/2021/CRP.1 de forma acelerada por falta de tiempo, en vista de las disposiciones de organización aprobadas en relación con la COVID-19, en que se asignaron 12 horas a la séptima reunión, en vez de las 18 horas habituales. El Grupo de Expertos estuvo de acuerdo con esa propuesta y también en transmitir a la Comisión las 63 conclusiones y recomendaciones convenidas que figuran en el anexo del presente informe.

20. También en su quinta sesión, el Grupo de Expertos examinó el tema 3 del programa, titulado “Examen de la labor futura del Grupo de Expertos”. Se expresaron opiniones divergentes al respecto, como queda reflejado en las declaraciones que figuran en la página web de la séptima reunión del Grupo de Expertos[1].

E. Asistencia

21. Asistieron a la reunión representantes de 111 Estados Miembros, 5 institutos de la red del programa de las Naciones Unidas en materia de prevención del delito y justicia penal, 3 entidades de las Naciones Unidas y 11 organizaciones intergubernamentales, así como representantes del mundo académico y del sector privado.

22. La lista de participantes figura en el documento UNODC/CCPCJ/EG.4/2021/INF/1/Rev.1.

F. Documentación

23. El Grupo de Expertos tuvo ante sí los siguientes documentos:

a) Programa provisional anotado (UNODC/CCPCJ/EG.4/2021/1);

b) Recopilación de todas las conclusiones y recomendaciones preliminares sugeridas por los Estados Miembros durante las reuniones del Grupo de Expertos

[1] Véase www.unodc.org/unodc/en/organized-crime/open-ended-intergovernmental-expert-group-to-conduct-a-comprehensive-study-of-the-problem-of-cybercrime_2021.html.

encargado de realizar un estudio exhaustivo sobre el delito cibernético celebradas en 2018, 2019 y 2020 (UNODC/CCPCJ/EG.4/2021/CRP.1).

III. Aprobación del informe

24. En su sexta sesión, celebrada el 8 de abril de 2021, el Grupo de Expertos aprobó el presente informe.

Anexo

Conclusiones y recomendaciones convenidas por el Grupo de Expertos para someter a examen de la Comisión de Prevención del Delito y Justicia Penal

Legislación y marcos

1. 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, cuando lo consideren necesario y adecuado, los Estados Miembros deberían considerar la posibilidad de adoptar una terminología coherente para describir las actividades cibernéticas delictivas en el plano nacional 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.

2. Los Estados Miembros deberían apoyar a la Oficina de las Naciones Unidas contra la Droga y el Delito (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.

3. 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: 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.

Tipificación

4. 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.

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

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

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

c) la interferencia ilícita en los datos y sistemas informáticos.

6. 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.

Aplicación de la ley e investigaciones

7. 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.

8. 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.

9. 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.

10. 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 ciberdelincuencia. 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, la privacidad, los derechos humanos y las libertades fundamentales. Además, los Estados Miembros deberían dedicar recursos a promulgar leyes nacionales que autoricen lo siguiente:

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

b) la cooperación internacional de las autoridades nacionales encargadas de hacer cumplir la ley.

Pruebas electrónicas[2] y justicia penal

11. 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.

12. 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.

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

14. La UNODC debería establecer un programa educativo dedicado a aumentar los conocimientos de las autoridades judiciales y el ministerio público de los Estados Miembros acerca de las medidas de lucha contra la ciberdelincuencia, especialmente en la esfera de la obtención de pruebas electrónicas, y a sensibilizarlos al respecto.

15. 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.

[2] Un Estado Miembro aclaró, en relación con el término “pruebas electrónicas”, que “electrónicas” se refería a la forma de transmisión o almacenamiento de datos y que podría incluir también, por ejemplo, las ondas de radio o la fibra óptica. Aclaró también que se quería hacer referencia a “información digital”, que consistía en unos y ceros, y no a “pruebas electrónicas”. Otro Estado Miembro indicó que las “pruebas electrónicas” incluían las pruebas digitales y las analógicas.

16. 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 mensajes de correo electrónico; 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.

17. Los Estados Miembros deberían establecer y aplicar marcos jurídicos, normas jurisdiccionales y otras disposiciones de procedimiento para permitir la investigación eficaz a nivel nacional del delito cibernético, así como una cooperación internacional efectiva a ese respecto, mediante una aplicación eficaz de la ley, que respete la soberanía nacional, y la protección de la privacidad y de todos los derechos humanos. Ello puede incluir:

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

b) la adopción de disposiciones sobre la localización nacional e internacional de las comunicaciones.

18. Los Estados Miembros deberían esforzarse por aumentar la cooperación en la obtención de pruebas electrónicas. A ese respecto, se les alienta a considerar, entre otras cosas, lo siguiente:

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

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

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

d) 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;

e) 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;

f) 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;

g) la celebración de talleres y seminarios para dar a conocer las mejores prácticas en la lucha contra la ciberdelincuencia.

Cooperación internacional

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

20. Deberían optimizarse los procedimientos de cooperación internacional para que se preste la máxima asistencia, dentro de las posibilidades que ofrezcan los marcos jurídicos nacionales, a las solicitudes de cooperación internacional relativas a la conservación de pruebas electrónicas y el acceso a archivos de conexión y a la información de registro de los usuarios de un modo que no vulnere los derechos humanos, las libertades fundamentales ni los derechos de propiedad.

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

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

23. Se exhorta a los países a que, para conservar e intercambiar pruebas electrónicas admisibles, se incorporen a redes autorizadas de profesionales, como las redes que operan de manera ininterrumpida, las redes especializadas en ciberdelincuencia y los canales de la Organización Internacional de Policía Criminal (INTERPOL) para la cooperación interpolicial ágil, y a que utilicen esas redes en mayor medida y las refuercen, así como también se les exhorta a que establezcan redes con entidades colaboradoras que tengan la misma estrategia, con vistas a intercambiar datos sobre asuntos de ciberdelincuencia, habilitar respuestas rápidas y minimizar la pérdida de pruebas esenciales. También se recomienda el uso de la cooperación interpolicial y otros métodos de cooperación oficiosa antes de acudir a los canales de asistencia judicial recíproca.

24. Los Estados Miembros deberían intercambiar información sobre la forma en que se están resolviendo en el plano nacional los problemas para acceder de manera oportuna a las pruebas digitales, con el fin de que otros Estados Miembros se beneficien de esas experiencias y aumenten la eficiencia y eficacia de sus propios procesos.

25. Los Estados Miembros deberían establecer prácticas que permitan transmitir y recibir solicitudes de asistencia judicial recíproca por medios electrónicos, a fin de reducir las demoras en la transmisión de documentos de un Estado a otro.

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

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

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

29. Se debería priorizar y reforzar la creación de capacidad y la asistencia técnica sostenibles para aumentar la capacidad en todas las esferas operacionales y fortalecer la capacidad de las autoridades nacionales para responder a la ciberdelincuencia, por ejemplo, mediante el establecimiento de redes, la celebración de reuniones y cursos de capacitación conjuntos, el intercambio de mejores prácticas, la facilitación de material de capacitación y la elaboración de plantillas para la cooperación. La creación de capacidad y la capacitación mencionadas deberían incluir una formación altamente especializada para los profesionales, que promueva, en particular, la participación de mujeres expertas, y se debería prestar atención a las necesidades de los legisladores y los encargados de formular políticas para tratar mejor las cuestiones relativas a la conservación de datos a efectos de hacer cumplir la ley. La creación de capacidad y la capacitación también deberían centrarse en desarrollar las aptitudes de las autoridades encargadas de hacer cumplir la ley, los investigadores y los analistas en ciencia forense en lo que respecta a la utilización de datos de código abierto para las investigaciones y a la cadena de custodia de las pruebas electrónicas, así como a la reunión y el intercambio de pruebas electrónicas en el extranjero. Otra esfera de prioridad en las actividades de creación de capacidad y capacitación debería ser desarrollar las aptitudes de jueces, fiscales, autoridades centrales y abogados para juzgar y tratar eficazmente los casos pertinentes.

30. La cooperación internacional es importante para reunir e intercambiar pruebas electrónicas en el contexto de las investigaciones transfronterizas y para responder rápida y eficazmente a las solicitudes de asistencia judicial recíproca relativas a la conservación y la obtención de pruebas electrónicas. Durante el proceso deben respetarse los principios de soberanía y reciprocidad.

31. Se alienta a la UNODC a que siga ofreciendo a los expertos gubernamentales nacionales programas de creación de capacidad y formación en la lucha contra la ciberdelincuencia, a fin de fortalecer la capacidad de detectar e investigar los delitos cibernéticos. Las actividades de creación de capacidad en esa esfera deberían abordar las necesidades de los países en desarrollo, centrarse en la vulnerabilidad de cada país a fin de prestar una asistencia técnica adaptada a sus circunstancias y promover el intercambio de los conocimientos más actualizados en favor de los profesionales y demás interesados.

32. La UNODC ha elaborado el Programa para Redactar Solicitudes de Asistencia Judicial Recíproca a fin de ayudar a los profesionales de la justicia penal a redactar dichas solicitudes. La Oficina también ha elaborado una guía práctica para la solicitud de pruebas electrónicas transfronterizas (Practical Guide for Requesting Electronic Evidence Across Borders), que está a disposición de los profesionales de los organismos de los Estados Miembros que la soliciten. Los países pueden beneficiarse de la utilización de esos instrumentos clave desarrollados por la UNODC.

33. Se pidió la participación activa de todos los Estados Miembros en la labor del comité especial encargado de elaborar una nueva convención.

34. Los Estados Miembros deberían considerar la posibilidad de invertir en fuerzas centralizadas especializadas en el delito cibernético y en dependencias tecnológicas regionales de investigación penal.

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

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

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

Prevención

38. Debe reconocerse que la prevención no es solo responsabilidad de los Gobiernos: también requiere la participación de todos los interesados pertinentes, incluidos los organismos encargados de hacer cumplir la ley, el sector privado —especialmente los proveedores de servicios de Internet—, las organizaciones no gubernamentales, las escuelas y los círculos académicos, además del público en general.

39. Se recomienda que el público tenga fácil acceso a instrumentos de prevención como plataformas en línea, archivos de audio e infografías en lenguaje sencillo, y a plataformas para presentar denuncias.

40. Se considera necesario elaborar una serie de políticas públicas de largo plazo en materia de prevención, que deberían incluir el desarrollo de campañas de sensibilización sobre el uso seguro de Internet.

41. Al prevenir y combatir el delito cibernético, los Estados deberían prestar especial atención a las cuestiones de la prevención y la erradicación de la violencia de género, en particular la violencia contra las mujeres y las niñas, y los delitos motivados por el odio.

42. Las actividades de prevención deben ser proactivas, periódicas, continuas y adecuadas para los grupos vulnerables.

43. Los Estados deberían impartir capacitación para magistrados y jueces especializados que se ocupan de los casos de delito cibernético, y proporcionar a los órganos de investigación instrumentos de alto rendimiento para rastrear las criptomonedas y hacer frente a su utilización con fines delictivos.

44. Se recomienda fomentar la capacidad colectiva de las instituciones competentes y cambiar la cultura de prevención para que deje de ser reactiva y se vuelva proactiva. También se recomienda establecer un mecanismo sólido para estimular y facilitar el intercambio de información de inteligencia sobre los posibles *modus operandi* delictivos.

45. Se alienta a los Estados Miembros a que sigan incluyendo medidas de prevención eficaces en los planos nacional e internacional y a que se centren en actividades proactivas, como la sensibilización sobre los peligros del delito cibernético, realizando campañas relativas específicamente a los *modus operandi*, como el *phishing* o los programas maliciosos (“programas secuestradores”), y dirigidas a diferentes grupos, como los jóvenes o las personas de edad. También se alienta a los Estados Miembros a que continúen centrándose en la probabilidad de enjuiciar y castigar a los delincuentes y en los esfuerzos por prevenir el delito descubriendo y desbaratando las actividades en curso de carácter ilícito perpetradas en línea. Los servicios de policía y de fiscalía deberían invertir en señalizar y descubrir las amenazas de la ciberdelincuencia y reaccionar a ellas. La colaboración entre el sector público y el privado es indispensable. Estas actividades de prevención no requieren leyes ni reglamentos adicionales.

46. Debido a la existencia de la “brecha digital”, algunos países en desarrollo carecen de capacidad para prevenir, detectar y combatir el delito cibernético, y son más vulnerables ante los desafíos que este plantea.

47. Se alienta encarecidamente a la UNODC a que siga prestando asistencia técnica para prevenir y combatir el delito cibernético a quienes la soliciten.

48. Se alienta a los Estados Miembros a que sigan incluyendo medidas de prevención eficaces en los planos nacional e internacional y a que se centren en actividades proactivas, como la sensibilización sobre los peligros del delito cibernético y la probabilidad de que los delincuentes sean enjuiciados y castigados, y en iniciativas para prevenir nuevos delitos descubriendo y desbaratando las actividades ilícitas que se llevan a cabo en línea.

49. Los países deberían reunir una amplia gama de datos que ayuden a comprender las tendencias, a fin de fundamentar y configurar las políticas contra el delito cibernético y las respuestas operacionales para combatirlo.

50. Al elaborar estrategias de prevención del delito cibernético se debería tener en cuenta también la protección de los derechos humanos.

51. La “capacidad de la justicia penal” debería ser otra esfera de atención de las estrategias nacionales contra el delito cibernético. La asistencia a los países en desarrollo debería ser una prioridad, a fin de fortalecer la capacidad de los organismos encargados de hacer cumplir la ley para prevenir el delito cibernético.

52. Los Estados deberían establecer programas de apoyo a las víctimas de delitos cibernéticos, o reforzar los existentes.

53. Los Estados deberían realizar estudios para medir los efectos del delito cibernético en las empresas, incluidas las medidas aplicadas, la capacitación de los empleados, los tipos de incidentes cibernéticos que les afectan y los costos relacionados con la recuperación tras los incidentes cibernéticos y su prevención.

54. Los Estados deberían apoyar a las empresas y comunidades en la labor de concienciar sobre los riesgos del delito cibernético, adoptar estrategias de mitigación y mejorar las prácticas cibernéticas, ya que ello puede tener importantes beneficios en materia de prevención en el futuro.

55. Se deberían estudiar atentamente los *modus operandi* de los ciberdelincuentes contemporáneos mediante el análisis de información de inteligencia y la investigación criminológica, a fin de asignar los recursos existentes de manera más eficaz y detectar las vulnerabilidades.

56. Los países deberían considerar la posibilidad de adoptar medidas específicas y adaptadas a necesidades concretas para mantener a los niños seguros cuando estén en línea. A tal fin, entre otras cosas, se debería velar por que los marcos jurídicos nacionales, los arreglos prácticos y los arreglos de cooperación internacional permitan la denuncia, detección, investigación, enjuiciamiento y disuasión del abuso y la explotación sexuales de los niños en Internet.

57. La industria es un asociado clave en la prevención de la ciberdelincuencia. Los países deberían considerar la posibilidad de aplicar mecanismos de cooperación con la industria, incluso en lo que respecta a la remisión a las autoridades nacionales competentes y la retirada de material delictivo perjudicial, incluido el relativo a la explotación sexual infantil y al material violento abominable.

58. Deberían publicarse directrices periódicas sobre la prevención de incidentes y darse a conocer a usuarios, organizaciones y demás interesados, de manera que estos puedan prevenir ciberincidentes que podrían dar lugar a actividades delictivas.

59. Los Estados deberían implicar a mujeres expertas en la prevención e investigación de los delitos cibernéticos.

60. Se deberían reunir experiencias nacionales y regionales de prevención para crear un repositorio multilateral que permita la difusión de buenas prácticas en diversos contextos.

61. Se debería generar mayor conciencia acerca de los marcos reguladores contra el ciberacoso y las amenazas de violencia o abuso en línea, y se debería prestar asistencia legislativa al respecto.

62. Se recomienda que los Estados inviertan en la creación de capacidad para mejorar las aptitudes de los funcionarios de todo el espectro del sistema de justicia penal, como medida preventiva eficiente de efecto disuasivo contra el delito cibernético.

63. La UNODC debería facilitar la divulgación de las mejores prácticas sobre medidas preventivas eficaces y satisfactorias contra el delito cibernético.