Naciones Unidas A/AC.291/4

Asamblea General

Distr. general
17 de noviembre de 2021
Español
Original: árabe/chino/español/
inglés

Comité Especial encargado de Elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos

Recopilación de las opiniones presentadas por los Estados Miembros sobre el ámbito de aplicación, los objetivos y la estructura (los elementos) de una convención internacional integral sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos

Nota de la Secretaría

Resumen

Como parte de los preparativos del primer período de sesiones del Comité Especial encargado de Elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos, la secretaría elaboró la presente nota con arreglo a las instrucciones de la Presidencia del Comité. En ella se incluyen las opiniones remitidas por los Estados Miembros sobre el ámbito de aplicación, los objetivos y la estructura (los elementos) de la nueva convención.

V.21-08423 (S) 100122 100122

Índice

I. Introducción

1. Como parte de los preparativos del primer período de sesiones del Comité Especial encargado de Elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos, el 11 de agosto de 2021 la Presidenta del Comité, Sra. Faouzia Boumaiza Mebarki (Argelia), invitó a los Estados Miembros a que presentaran sus opiniones sobre el ámbito de aplicación, los objetivos y la estructura (los elementos) de la nueva convención. El plazo fijado para presentar esas opiniones era el 29 de octubre de 2021, aunque después se prorrogó hasta el 5 de noviembre de 2021.

2. Además, la Presidenta indicó a la secretaría que recopilase las opiniones que recibiera y las hiciera traducir a los seis idiomas oficiales de las Naciones Unidas para que estuvieran disponibles en el primer período de sesiones del Comité Especial.

3. La presente nota fue elaborada por la secretaría conforme a las instrucciones de la Presidencia y en ella figuran las opiniones remitidas por los Estados Miembros sobre el ámbito de aplicación, los objetivos y la estructura (los elementos) de la nueva convención.

II. Opiniones remitidas por los Estados Miembros

Australia

[Original: inglés]
[29 de octubre de 2021]

Australia acoge con beneplácito la oportunidad de presentar su opinión sobre el ámbito de aplicación, la estructura y los objetivos de una nueva convención internacional sobre la ciberdelincuencia. La nueva convención ofrece una oportunidad incomparable de lograr un consenso amplio sobre la cooperación internacional contra la ciberdelincuencia, ya que permitiría a los Estados combatir mejor esa amenaza omnipresente, que cambia de forma constante.

La nueva convención solo será útil si recibe un apoyo generalizado de la mayoría de los Estados Miembros, lo que depende de que se llegue a un acuerdo de consenso mediante conversaciones celebradas de buena fe bajo los auspicios del Comité Especial encargado de Elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos, creado en virtud de las resoluciones de la Asamblea General 74/247 y 75/282. Con ese fin, Australia está comprometida con la celebración de un proceso abierto, inclusivo y transparente en el que participen múltiples interesados, proceso que presenta la probabilidad más alta de que los Estados logren llegar a un resultado aceptable para el mayor número posible de Estados. Ello concuerda con los principios expuestos en las anteriores comunicaciones de Australia al Comité Especial, así como con las comunicaciones conjuntas en las que ha participado nuestro país. Australia aprovecha esta oportunidad para reiterar los mensajes transmitidos en esas comunicaciones.

La ciberdelincuencia supone una amenaza para todos los Estados, pero resulta especialmente difícil para los Estados pequeños. Mantener una cooperación internacional eficaz en materia de ciberdelincuencia reviste especial importancia para los pequeños Estados insulares en desarrollo, con el fin de ayudarlos a mejorar su capacidad interna de combatir las actividades de ciberdelincuencia transnacional. Es imprescindible que esos Estados puedan participar de manera significativa en la labor del Comité Especial. Australia está comprometida a asegurar que los países insulares del Pacífico cuenten con oportunidades adecuadas para participar en esa labor. Australia acoge con agrado la decisión de apoyar la participación híbrida (en persona y en línea) en los períodos de sesiones del Comité Especial

y pone de relieve la importancia de que las delegaciones más pequeñas cuenten con tiempo suficiente para prepararse y participar.

Las entidades del sector privado tienen una función excepcional e inestimable que cumplir para hacer frente a la ciberdelincuencia. Por tanto, para alcanzar su objetivo, en la labor del Comité Especial se deberán tener en cuenta los valiosos conocimientos especializados que proporcionan las partes interesadas del sector privado. Los Estados también deberían ser receptivos a los amplios conocimientos e ideas que otros actores no estatales, como las organizaciones de la sociedad civil, las instituciones académicas y los órganos intergubernamentales, pueden aportar al debate sobre la manera óptima de combatir la ciberdelincuencia. Para que los debates estén bien fundamentados y se obtengan resultados efectivos, el Comité Especial debería otorgar a esos grupos tantas oportunidades como sea posible para que puedan realizar contribuciones.

Ámbito de aplicación

Habida cuenta del breve plazo disponible para las negociaciones, los Estados disponen de tiempo limitado para alcanzar acuerdos sobre las numerosas cuestiones que comprende una nueva convención. Se debe definir claramente el ámbito de aplicación de la convención, el cual debería circunscribirse estrictamente a la respuesta de la justicia penal a la ciberdelincuencia. No debería ocuparse de cuestiones de ciberseguridad más amplias que ya se examinan en otros foros.

Para agilizar nuestra labor, los Estados deberían centrar la atención en las esferas en las que es necesario adoptar enfoques comunes contra la ciberdelincuencia. En su labor, el Comité Especial debería emplear conceptos y términos relacionados con la ciberdelincuencia y la cooperación internacional en materia de justicia penal que la comunidad internacional ya entiende bien. No es necesario “reinventar la rueda” ni resulta conveniente generar ambigüedad.

Por consiguiente, la nueva convención debería inspirarse en gran medida en la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y en la Convención de las Naciones Unidas contra la Corrupción, así como en otros conceptos que se han consensuado en los congresos de las Naciones Unidas sobre prevención del delito y justicia penal y en otros foros de las Naciones Unidas, según proceda. Deberían tomarse como referencia instrumentos internacionales eficaces existentes que los Estados ya han aprobado a nivel internacional y regional, como el Convenio sobre la Ciberdelincuencia del Consejo de Europa, y deberá evitarse que se socaven normas vigentes establecidas en esos acuerdos. Esto concuerda con el mandato otorgado por la Asamblea General en su resolución 74/247, en la que la Asamblea instó al Comité Especial a que en su labor tuviera plenamente en cuenta los instrumentos internacionales y las iniciativas existentes en los planos nacional, regional e internacional.

En particular, en la convención se debería seguir utilizando el término “ciberdelincuencia”. Este es un concepto que se comprende en general y que se ha usado en innumerables documentos de las Naciones Unidas, entre ellos, los documentos finales de los Congresos de las Naciones Unidas sobre Prevención del Delito y Justicia Penal 12º, 13º y 14º, varias resoluciones de la Asamblea General (especialmente la resolución 65/230) y muchas otras resoluciones e informes de la Comisión de Prevención del Delito y Justicia Penal y el Consejo Económico y Social.

Elementos del tratado (estructura y objetivos)

Tipificación

La nueva convención ofrece la oportunidad de mejorar sustancialmente la cooperación internacional en materia de ciberdelincuencia. La existencia de normas armonizadas

respecto de un conjunto básico de delitos cibernéticos aumentará la capacidad de los Estados de responder a la ciberdelincuencia a nivel mundial, regional e interno.

Con ese fin, Australia opina que en la convención se debería aplicar un enfoque centrado en los tipos de conducta delictiva que la ciberdelincuencia ha alterado de manera sustancial. Normalmente, el derecho penal interno de los Estados es más que suficiente para definir delitos conocidos como la violación de domicilio, el vandalismo, el robo, los delitos relacionados con estupefacientes y los delitos violentos. No es necesario que la convención vuelva a definir esos delitos tan solo porque en su comisión entren en juego una computadora o un sistema informático.

La nueva convención debe incluir normas nuevas para tipificar los delitos que solo se pueden cometer empleando sistemas de la información y las comunicaciones, delitos que reciben diversas denominaciones, entre ellas, “ciberdelincuencia pura” y “delitos basados en la cibernética”. Son delitos que no existían antes de que aparecieran las redes de información y comunicaciones, y a menudo el derecho penal interno de los Estados es insuficiente o no se puede aplicar de manera sistemática a esos delitos. En ese sentido, la existencia de unas normas armonizadas para tipificar delitos ofrecerá a los Estados ventajas notables, tanto en lo que respecta a sus propias actividades internas de lucha contra la ciberdelincuencia como en lo que se refiere a facilitar una mayor cooperación internacional.

De manera similar, Australia considera que hay algunos delitos “tradicionales” cuya extensión, escala y facilidad de comisión se han visto incrementadas drásticamente por la velocidad, el anonimato y la amplitud de alcance que permiten las redes de información y comunicaciones. Estos se denominan a menudo delitos “facilitados por la cibernética”. La convención debería tratar esos delitos de manera juiciosa, mediante la formulación de un marco claro para intentar establecer por qué determinados delitos se ven alterados por un “elemento cibernético” de manera tan notable como para que se precise una nueva norma internacional armonizada que coloque esa conducta por encima de los delitos “tradicionales”. No es necesario que en la Convención se defina una nueva categoría de delito por cada delito ya existente que pueda presentar un elemento cibernético, y menos aún si este no altera de manera significativa ni la gravedad ni el alcance del acto tipificado.

Australia considera que hay dos candidatos evidentes a la categoría de delitos facilitados por la cibernética que se deberían incluir en la convención: la explotación y los abusos sexuales a niños en línea, que suponen una grave amenaza, y el fraude y el robo facilitados por la cibernética, incluida la extorsión vinculada a programas secuestradores, delitos que han aumentado de manera notable y generalizada. Australia está dispuesta a escuchar argumentos en favor de examinar también otros delitos facilitados por la cibernética, pero, por los motivos expuestos, en la convención se debería aplicar un enfoque restrictivo en lo que respecta a crear cualquier categoría de delito nueva.

En la convención también se debería prestar la debida atención a los delitos determinantes y a la responsabilidad subsidiaria por los delitos basados en la cibernética o facilitados por esta. Ello debería incluir la habitual extensión de la responsabilidad penal prevista en instrumentos como la Convención contra la Delincuencia Organizada y la Convención contra la Corrupción. Dada la función que cumple la tecnología en cuanto a facilitar la ciberdelincuencia, también se debería considerar la posibilidad de incluir en la convención una norma penal armonizada para los delitos que comporten la producción, la adquisición o el suministro de tecnología y programas informáticos adaptados sola o primordialmente para la comisión de delitos cibernéticos.

La ciberdelincuencia es un ámbito en que se producen rápidas transformaciones y los ciberdelincuentes tratan constantemente de aplicar nuevas tecnologías y metodologías para ampliar sus actividades y eludir la acción de la justicia. Para contrarrestar esa dinámica, en la convención se debe procurar redactar las normas que tipifiquen delitos de un modo neutro desde los puntos de vista tecnológico y metodológico, a fin de que el tratado conserve su pertinencia y eficacia en el futuro.

Medidas procesales para combatir la ciberdelincuencia

El derecho procesal es un elemento fundamental en la investigación y el enjuiciamiento de los delitos cibernéticos. La convención debería proporcionar un marco claro de medidas procesales que garantizasen que los organismos encargados de hacer cumplir la ley puedan obtener las pruebas necesarias para combatir la ciberdelincuencia. El ámbito de aplicación de cualquier marco de medidas procesales debería servir de respaldo a la legislación de cada país, la cual debe ser clara y suficientemente sólida, de manera que los organismos encargados de hacer cumplir la ley u otras autoridades competentes puedan hacer frente a los retos que plantea la ciberdelincuencia, entre otras maneras, mediante la detección, la desarticulación, la prevención, la investigación y el enjuiciamiento.

Además, las medidas procesales deberían adecuarse a las características de los datos electrónicos y garantizar que los organismos encargados de hacer cumplir la ley y otras autoridades competentes puedan obtener esos datos con rapidez y eficacia para que las metodologías y las prácticas delictivas seguidas en el ciberespacio no minen la labor de reunión de pruebas por parte de las autoridades. Entre los tipos de medidas procesales previstos podrían figurar las facultades para efectuar registros e incautaciones, las facultades relacionadas con la obtención de datos (por ejemplo, el acceso a comunicaciones almacenadas y las actividades de interceptación) y las órdenes o solicitudes urgentes o de emergencia para la revelación de esos datos. Las medidas procesales deben sustentarse en limitaciones estrictas y salvaguardias sólidas que protejan adecuadamente los derechos humanos y el estado de derecho.

Los Estados probablemente deberán estudiar cómo dar cabida en la nueva convención a las prácticas de los distintos Estados en lo que respecta a la reunión de datos electrónicos en las distintas jurisdicciones.

Cooperación internacional y asistencia técnica

La inmensa mayoría de los delitos cibernéticos son transnacionales. Para que los Estados puedan investigar y enjuiciar con eficacia a los ciberdelincuentes es crucial la cooperación internacional, la cual debe apoyarse en una tipificación armonizada.

En los últimos decenios la comunidad internacional ha logrado avances notables en lo que respecta a la cooperación internacional en la esfera de la justicia penal y ha elaborado instrumentos eficaces en una gama de tratados internacionales vigentes que rigen la asistencia judicial recíproca, la extradición y otras formas de cooperación internacional. Por ejemplo, las disposiciones de la Convención contra la Delincuencia Organizada y la Convención contra la Corrupción ofrecen una base excelente para esa cooperación y han sido aprobadas de manera casi universal.

La nueva convención debería inspirarse tanto como sea posible en las disposiciones similares de la Convención contra la Delincuencia Organizada y la Convención contra la Corrupción que guardan relación con la asistencia judicial recíproca, la extradición, el traslado de reclusos y la recuperación del producto del delito. Esas disposiciones tienen una eficacia probada y gozan de un amplio respaldo internacional. En consonancia con el mandato establecido en la resolución 74/247 de la Asamblea General, también se debería velar por que la nueva convención complementase y no minase otros mecanismos existentes de cooperación internacional en materia de justicia penal.

Otros regímenes internacionales y regionales ofrecen marcos eficaces de cooperación internacional contra la ciberdelincuencia que se sustentan en limitaciones estrictas y salvaguardias sólidas. La nueva convención debería basarse en esos regímenes tanto como sea posible. El principal de ellos es el Convenio sobre la Ciberdelincuencia del Consejo de Europa, que sigue ofreciendo una base eficaz para la cooperación internacional entre un gran número de Estados de todas las regiones del mundo.

Aparte de la cooperación internacional, la nueva convención debería impulsar notablemente las actividades dedicadas a mejorar la capacidad internacional de combatir la ciberdelincuencia. En su redacción se debería reafirmar la función principal que desempeña la Oficina de las Naciones Unidas contra la Droga y el Delito en lo que se refiere a prestar asistencia técnica y crear capacidad, lo que incluye la coordinación del Programa Mundial contra el Delito Cibernético.

Salvaguardias para proteger y promover los derechos humanos

Por su misma naturaleza, el acceso de los Estados a los datos electrónicos y de telecomunicaciones de las personas repercute en los derechos individuales. La convención debe reafirmar que, en sus actividades dedicadas a combatir la ciberdelincuencia, los Estados tienen la responsabilidad de promover y proteger los derechos humanos de las personas en consonancia con las normas internacionales de derechos humanos.

Se deben seguir protegiendo adecuadamente el derecho a la privacidad y los derechos a la libertad de opinión, de expresión y de asociación, en consonancia con las normas internacionales vigentes. Otros derechos que también se deben proteger son el derecho a un juicio imparcial, lo que incluye la igualdad ante la ley, así como el derecho a no ser sometido a torturas ni a penas o tratos inhumanos o degradantes, a detenciones arbitrarias ni a sufrir discriminación. La comunidad internacional ha reafirmado en repetidas ocasiones que esos derechos deben respetarse tanto en línea como fuera de Internet, y en la convención se debería reiterar la responsabilidad que tienen los Estados de respetar esos derechos en el transcurso de sus actividades de lucha contra la ciberdelincuencia.

Estructura y método de trabajo

Una vez que los Estados hayan tenido la ocasión de expresar su opinión respecto del ámbito de aplicación de la convención, en el primer período de sesiones de negociación, que se celebrará en enero de 2022, Australia prevé que se alcanzará con celeridad un consenso sobre la estructura de la convención.

Después de que los Estados hayan expresado su opinión sobre el ámbito de aplicación, la estructura y los objetivos de la nueva convención, en enero de 2022, Australia propone que se invite a los Estados a presentar propuestas de cláusulas para incluirlas dentro de cada elemento estructural de la nueva convención (por ejemplo, propuestas sobre la tipificación y la cooperación internacional). A continuación, la Presidencia, en consulta con la Mesa si es necesario, debería trabajar para sintetizar las diversas propuestas en un proyecto de texto que, seguidamente, los Estados podrían negociar examinando cada grupo de cláusulas según el orden fijado en el plan de trabajo establecido por el Comité Especial en su primera sesión.

Tras las negociaciones iniciales sobre cada elemento de la estructura, la convención podría seguir negociándose en conjunto, nuevamente según el plan de trabajo establecido por el Comité Especial en su primera sesión y administrado posteriormente por la Presidencia.

Brasil

[Original: inglés]
[29 de octubre de 2021]

Como muchos otros países, el Brasil está sufriendo la ciberdelincuencia, un fenómeno cuya frecuencia y complejidad están en auge. El que varios delitos se hayan trasladado a plataformas digitales obliga a actuar con resolución para actualizar la respuesta normativa y de las fuerzas del orden adecuándola a las amenazas planteadas, y ello incluye la esfera internacional. La amplitud geográfica y velocidad operacional de esos delitos ponen a prueba los mecanismos tradicionales de aplicación de la ley y de cooperación jurídica a nivel mundial.

Los desafíos son colosales. Los proveedores de servicios de Internet, que poseen información importante necesaria para investigar los delitos cibernéticos y reunir pruebas electrónicas, a menudo tienen su sede física en un país, prestan servicios en distintos continentes y almacenan su información en servidores localizados en cualquier otro lugar del planeta. En ese contexto, los organismos encargados de hacer cumplir la ley tienen dificultades para determinar quién tiene competencia sobre los datos y acceso directo a ellos y para dirigirse debidamente a la autoridad competente.

Lograr una coordinación internacional de las jurisdicciones que esté cohesionada es un paso necesario para el enjuiciamiento de los delitos cibernéticos. Se necesita más y mejor cooperación. Para desarticular eficazmente la ciberdelincuencia se precisa un medio de cooperación ágil y directo en el que los organismos encargados de hacer cumplir la ley puedan intercambiar de manera oportuna pruebas de distintas causas en las que esté involucrado un mismo grupo delictivo.

El Brasil está participando plenamente en la negociación de una convención amplia sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos. Esta es una oportunidad singular de fijar unas normas comunes de cooperación para hacer frente a un asunto que es esencialmente transnacional mediante el aprovechamiento de las mejores tradiciones y prácticas a ese respecto.

Desde el punto de vista del Brasil, para que la futura convención pueda estar a la altura de los desafíos descritos deberá incluir los elementos siguientes en lo que a sus objetivos, ámbito de aplicación y estructura se refiere.

Objetivos

El objetivo principal de la convención debería ser proporcionar herramientas específicas para la cooperación internacional, de manera que los Estados partes puedan obtener oportunamente pruebas y otra información que contribuyan a investigar y enjuiciar delitos cibernéticos. Pese al mérito que posee ese objetivo primordial por sí solo, sería ideal que el instrumento cumpliese otros dos objetivos: a) el establecimiento de obligaciones mínimas relativas a la tipificación de delitos (derecho penal sustantivo) en cada jurisdicción de los Estados partes; y b) el establecimiento de obligaciones mínimas que hagan posible una respuesta, una investigación y un enjuiciamiento oportunos (derecho procesal penal) en cada jurisdicción de los Estados partes.

El Brasil apoya plenamente la idea de que se elabore una convención universal. Somos conscientes de las dificultades que entraña negociar un instrumento que contenga unas normas mínimas de tipificación, sobre todo al tratarse de un fenómeno tan moderno y cambiante. Con todo, existen precedentes de logros en ese sentido. En otras esferas penales, como en el caso de los tratados universales vigentes en materia de delito, las negociaciones llegaron a buen puerto e hicieron posible que la mayor parte del planeta se comprometiese a cumplir unas normas sustantivas mínimas. El debate no debería partir de la suposición de que existe una antítesis entre el ámbito geográfico y el alcance de la tipificación, sino del entendimiento de que las negociaciones mismas serán el método más seguro para determinar cuál es el consenso mínimo posible con respecto al derecho penal sustantivo en materia de ciberdelincuencia. Por restringido que sea, un consenso mínimo sobre la tipificación —que esté bien fundado en conceptos neutros y genéricos— podría limitar las opciones de los ciberdelincuentes al escoger una jurisdicción, facilitar el intercambio de experiencias y reducir las disensiones de índole normativa entre los países que, para cooperar, exigen que se aplique el principio de la doble incriminación.

La puntualidad de la cooperación internacional dependerá siempre de los instrumentos procesales que tengan a su disposición los investigadores, fiscales y jueces de las jurisdicciones más diversas. Los instrumentos tradicionales de cooperación judicial, como las comisiones rogatorias y el reconocimiento de sentencias extranjeras, no bastan por sí solos en ningún lugar para garantizar una reacción adecuada a la ciberdelincuencia.

El carácter transnacional y la inestabilidad extrema de ese fenómeno requieren de una normalización procesal, aun cuando esta sea tan flexible y genérica como sea necesario para dar cabida a todas las singularidades de los ordenamientos jurídicos nacionales en juego. No obstante, el eje de esa normalización procesal debería ser el establecimiento de unas normas mínimas para hacer posible el aseguramiento de pruebas electrónicas, medida que se activaría por una vía internacional ágil y directa; de lo contrario no permitirá la identificación de los delincuentes, sobre todo en los casos de delincuencia organizada.

Ámbito de aplicación

La convención debería servir como base del intercambio de pruebas y datos en relación con a) delitos contra sistemas informáticos; y b) cualquier delito que se cometa por medios electrónicos. Lo ideal sería que abarcase los datos electrónicos relacionados con las conexiones, el contenido y los abonados.

Además, la convención debería permitir a las partes presentar solicitudes de cooperación internacional (para el aseguramiento expedito de datos electrónicos y para recibir asistencia judicial recíproca) y transmitir información espontáneamente a otras jurisdicciones. Se tendría que dedicar un capítulo a la conformación de una red internacional de profesionales cuya función sería responder a los casos urgentes. Ese mecanismo operacional refuerza la idea de que una convención de esas características requiere de la creación de un órgano decisorio que supervise y examine su aplicación.

Tratándose de un instrumento marco, en el tratado se podría plantear la posibilidad de negociar protocolos que sirviesen como instrumentos adicionales, los cuales profundizarían la cooperación respecto de tipos específicos de delitos cibernéticos.

Por consiguiente, la convención debería constituir un instrumento para la aplicación práctica del derecho penal, instrumento que no ahondaría en políticas en materia de paz y seguridad internacionales, ciberdefensa ni cuestiones relativas a la estructura o la gobernanza de Internet en el plano nacional, regional o mundial.

Estructura

A la luz de las consideraciones precedentes, el Brasil considera que la convención debería tener la siguiente estructura:

Capítulo I. Tipificación.

Capítulo II. Derecho procesal penal que facilite una investigación y un enjuiciamiento oportunos.

Capítulo III. Cooperación internacional.

A. Aseguramiento expedito de los datos en formato electrónico.

B. Asistencia judicial recíproca.

C Transmisión espontánea de información.

Capítulo IV. Red de cooperación.

Capítulo V. Mecanismo de seguimiento para supervisar y examinar la aplicación.

Canadá

[Original: inglés]
[1 de noviembre de 2021]

Mediante la presente comunicación, el Canadá responde a la invitación remitida el 11 de agosto por la secretaría del Comité Especial encargado de Elaborar una Convención

Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos, en la que solicitó a los Estados Miembros que le hicieran llegar su opinión sobre el ámbito de aplicación, los objetivos y la estructura (los elementos) de la nueva convención.

Para preparar las siguientes observaciones, el Canadá se ha inspirado en la importante labor que se ha efectuado en la esfera de la ciberdelincuencia en las Naciones Unidas a lo largo de más de 20 años bajo los auspicios de la Comisión de Prevención del Delito y Justicia Penal, especialmente la llevada a cabo por el Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético, de carácter intergubernamental, por la Oficina de las Naciones Unidas contra la Droga y el Delito, por medio de su Programa Mundial contra el Delito Cibernético, y en los congresos de las Naciones Unidas sobre prevención del delito y justicia penal. Esas iniciativas han preparado el terreno para la elaboración de una convención de las Naciones Unidas que debería centrarse exclusivamente en la lucha contra la ciberdelincuencia y no ocuparse de la ciberseguridad, la cibergobernanza ni otras cuestiones conexas que es mejor examinar en otros foros de las Naciones Unidas.

En consonancia con la resolución 75/282 de la Asamblea General y con sus anteriores comunicaciones al Comité Especial, el Canadá desea reiterar que la negociación de la nueva convención deberá ser un proceso transparente e inclusivo que dé a la sociedad civil y a otras partes interesadas pertinentes una oportunidad significativa de participar.

Ámbito de aplicación

La nueva convención debería proporcionar un marco para combatir la ciberdelincuencia y los delitos graves que se cometen frecuentemente utilizando sistemas informáticos, el cual debería incluir los siguientes elementos:

a) disposiciones relativas a los delitos cibernéticos sustantivos y a la investigación y el enjuiciamiento de los delitos cibernéticos y de otros delitos graves que se cometen frecuentemente utilizando sistemas informáticos;

b) disposiciones sobre la cooperación internacional en relación con lo anterior, así como sobre la obtención de pruebas electrónicas de otros delitos;

c) disposiciones que incluyan medidas encaminadas a prevenir la ciberdelincuencia; y

d) disposiciones que incluyan medidas que alienten a los Estados Miembros y otras partes interesadas a realizar iniciativas de asistencia técnica y creación de capacidad de forma continua.

Los elementos de la nueva convención deberán ser compatibles con las obligaciones internacionales en materia de derechos humanos, especialmente en lo que respecta a las libertades de expresión, de opinión y de asociación, así como al derecho a no ser objeto de injerencias ilícitas ni arbitrarias en la vida privada.

Objetivos

La nueva convención debería tener los siguientes objetivos:

a) partiendo de una concepción común, establecer una base de referencia para los delitos sustantivos, las facultades procesales y la cooperación internacional contra la ciberdelincuencia;

b) velar por que las disposiciones estén redactadas en términos neutros desde el punto de vista tecnológico para que no queden obsoletas o sean imposibles de ejecutar a medida que evolucionen las tecnologías;

c) promover y facilitar la cooperación internacional en la lucha común contra la ciberdelincuencia;

d) establecer la autoridad para reunir, obtener y compartir pruebas electrónicas de otros delitos;

e) eliminar los refugios seguros para quienes cometan delitos cibernéticos;

f) garantizar la compatibilidad con las obligaciones internacionales en materia de derechos humanos, especialmente en lo que respecta a la libertad de expresión, de opinión y de asociación, así como al derecho a no ser objeto de injerencias ilícitas o arbitrarias en la vida privada;

g) garantizar la coherencia con los tratados vigentes de las Naciones Unidas en la esfera de la prevención del delito y la justicia penal, especialmente la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y la Convención de las Naciones Unidas contra la Corrupción, y tener en cuenta los instrumentos multilaterales cuya utilidad en la lucha contra la ciberdelincuencia ya ha quedado demostrada, sobre todo el Convenio sobre la Ciberdelincuencia del Consejo de Europa; y

h) apoyar a los Estados Miembros para que fortalezcan su capacidad de hacer frente a la ciberdelincuencia por medio de la asistencia técnica y la creación de capacidad.

Estructura

El Canadá considera importante que, además de incluir definiciones claras y disposiciones finales, la estructura de la nueva convención contenga los cinco elementos siguientes:

a) Disposiciones sobre los delitos sustantivos que exijan que los Estados Miembros adopten las medidas legislativas y de otra índole que sean necesarias para:

i) tipificar como delitos los actos que atenten contra la confidencialidad, la integridad y la disponibilidad de sistemas, redes y datos informáticos, así como el uso indebido de esos sistemas, redes y datos; y

ii) garantizar que su derecho penal regule de manera adecuada los delitos tradicionales que se especifiquen y que se cometan frecuentemente utilizando sistemas informáticos, por ejemplo, la distribución de pornografía en que se utilizaran niños.

b) Disposiciones procesales que exijan que los Estados Miembros adopten las medidas legislativas y de otra índole que sean necesarias para establecer la autoridad a fin de conservar y obtener pruebas electrónicas de delitos que estén alojadas en sistemas informáticos situados en múltiples jurisdicciones o en jurisdicciones extranjeras o desconocidas. Aunque en la nueva convención se deberían prever facultades de investigación más generales, como las de registro e incautación y las órdenes de presentación, también se deberían prever herramientas de investigación más especializadas para hacer frente a la velocidad a la que pueden cometerse los delitos y a la fugacidad y la volatilidad de las pruebas electrónicas. Esas disposiciones deberían estar supeditadas a salvaguardias que garantizasen que las actividades de aplicación de la ley respeten las obligaciones internacionales en materia de derechos humanos.

c) La cooperación internacional es importante para combatir la ciberdelincuencia. Es necesario que la nueva convención incluya mecanismos que faciliten la cooperación internacional tanto oficial como oficiosa para detectar, investigar y enjuiciar los delitos cibernéticos, así como para obtener pruebas electrónicas de otros delitos.

d) Es necesario que la nueva convención contenga medidas preventivas similares a las expuestas en la Convención contra la Delincuencia Organizada y la Convención contra la Corrupción, por ejemplo, disposiciones sobre iniciativas educativas y de sensibilización. Las alianzas de múltiples partes interesadas y la sociedad civil pueden cumplir una función esencial y ello se debería reflejar en esas disposiciones.

e) La nueva convención debería alentar a los Estados Miembros a fortalecer su capacidad de hacer frente a la ciberdelincuencia por medio de la asistencia técnica y la creación de capacidad. Con ese fin, se podrían incluir disposiciones que:

i) apoyaran la participación de múltiples partes interesadas;

ii) alentaran la colaboración con la Oficina de las Naciones Unidas contra la Droga y el Delito y su Programa Mundial contra el Delito Cibernético a fin de mejorar las aptitudes de los profesionales y las autoridades centrales en lo que respecta al uso de la tecnología para facilitar la cooperación internacional en la lucha contra la ciberdelincuencia; y

iii) desarrollen los programas de capacitación para investigadores y fiscales y apoyen el intercambio de información y experiencias con las partes interesadas pertinentes.

Chile

[Original: inglés]
[5 de noviembre de 2021]

El Gobierno de Chile se complace en responder a la invitación enviada a los Estados Miembros para que presentasen su opinión sobre el ámbito de aplicación, los objetivos y la estructura (los elementos) de la nueva convención, respecto de la aplicación de las resoluciones 74/247 y 75/282 de la Asamblea General.

Chile considera que la nueva convención no debería entrar en contradicción con otros tratados o acuerdos ya existentes en materia de ciberdelincuencia. Debería basarse en la cooperación internacional y en la asistencia técnica como fundamentos del enfoque multilateral para combatir los delitos cibernéticos. Se deben considerar de igual importancia las opiniones de todos los países, a fin de que el proceso sea abierto, inclusivo y transparente y en él participen múltiples partes interesadas.

1. Aspectos generales

a) *Jurisdicción*. La nueva convención supone una oportunidad excelente de examinar esta cuestión, que es la base de muchos de los instrumentos procesales que pueden utilizarse.

b) Las definiciones deben redactarse de manera amplia para preservar su pertinencia y aplicabilidad en un contexto de rápida transformación tecnológica. Deberán incluirse definiciones, entre otras cosas, de los distintos tipos de datos.

2. Derecho penal sustantivo

a) *Inclusión del delito de recepción de datos informáticos*. Aunque en algunos países se tiene una concepción restringida de este tipo delictivo, parece apropiado incluir un acto ilícito que comporte esa clase de conducta cuando los “bienes” robados sean datos informáticos y quien los almacenara no pudiera desconocer que el origen de los datos era ilícito.

b) En lo que respecta a la autoría y la participación, parece adecuado hacer frente de manera específica a la colaboración prestada por la persona receptora del dinero o de los títulos sustraídos de manera ilícita mediante fraude informático, dado que, si se tienen en cuenta las particularidades y las dificultades investigativas que presenta esta clase de delitos en la gran mayoría de los casos, es pertinente dar un tratamiento especial al enjuiciamiento de quienes, por norma general, constituyen el primer eslabón de la cadena delictiva. Por tanto, atendiendo a su participación, es apropiado elevar su situación a la de autores del fraude, sin perjuicio de la posibilidad de que se ofrezca una rebaja de las sanciones en el caso de que cooperen eficazmente en la captura de los demás delincuentes informáticos.

3. Normas de derecho procesal

a) Es adecuado examinar nuevas ideas y herramientas de trabajo que las autoridades podrían aplicar para detectar figuras delictivas que se estuvieran elaborando o que vayan a cometerse en Internet, así como la manera más eficaz de hacer frente a esa clase de delito.

b) Parece adecuado analizar el equilibrio que se debe mantener entre, por un lado, la debida y necesaria protección de los ciudadanos y sus datos personales y, por el otro, la investigación de los delitos, puesto que la sobreprotección de esa clase de información podría tener consecuencias en el desarrollo de los procedimientos de investigación que hacen posible el enjuiciamiento penal, de manera correcta y oportuna, de ese tipo de delito, el cual se beneficia del anonimato, del carácter transnacional y de la falta de rastreabilidad que comporta ese tipo de conducta.

4. Capítulo sobre la cooperación internacional

a) Es importante establecer principios en relación con la asistencia judicial recíproca en los asuntos penales.

b) Los países deberían analizar las maneras de contribuir a que los investigadores y fiscales que se ocupan de los delitos cibernéticos intercambien la información de manera oportuna y segura.

c) Los países deberían colaborar estrechamente entre sí, en consonancia con sus respectivos ordenamientos jurídicos y administrativos, con miras a aumentar la eficacia de las medidas de cumplimiento de la ley orientadas a combatir la ciberdelincuencia. Cada país debería adoptar medidas eficaces para establecer vías de comunicación entre sus autoridades, organismos y servicios competentes a fin de facilitar el intercambio seguro y rápido de información sobre todos los aspectos de los delitos cibernéticos.

d) La transmisión electrónica de asistencia judicial recíproca debería considerarse una opción válida y permanente, en lugar de reservarse para las emergencias.

e) Conservación y entrega de datos.

f) Se debería analizar la función positiva que cumplen las redes que operan de manera ininterrumpida y considerarlas una contribución innovadora a la cooperación internacional.

g) Regulación de las situaciones de emergencia.

h) Los países deberían definir entre todos cuál es la “brecha digital” que existe entre países, dado que algunos de ellos carecen de capacidad y medios para prevenir, detectar y combatir la ciberdelincuencia y son más vulnerables a los desafíos que esta plantea.

5. Herramientas especiales para la cooperación internacional

a) Entrega de datos por los proveedores de servicios de Internet y su relación con los Estados.

b) Acceso transfronterizo a los datos.

c) Técnicas de investigación especiales: agentes encubiertos en línea, equipos conjuntos de investigación e investigaciones conjuntas, entre otras cosas.

6. Prevención

a) Para prevenir la ciberdelincuencia es necesaria la participación de diversas partes interesadas, entre ellas, los Gobiernos, los organismos encargados de hacer cumplir la ley, el sector privado, las organizaciones internacionales, las organizaciones no gubernamentales y las entidades del mundo académico.

b) Se deberían promover estrategias de prevención que estuvieran centradas en las víctimas e hicieran frente a los delitos cibernéticos interpersonales.

c) Los países deberían considerar la posibilidad de aplicar mecanismos de cooperación con los especialistas del sector, entre ellos, la remisión de casos a las autoridades nacionales competentes y la retirada del material delictivo y perjudicial, por ejemplo, las imágenes de explotación sexual de niños y otros tipos de material violento que sea abominable.

7. La perspectiva de género en el contexto de la convención sobre la ciberdelincuencia

a) Se debería incluir una perspectiva de género al aplicar las disposiciones de la convención y evaluar sus efectos, así como realizar un análisis con perspectiva de género respecto del uso de la tecnología de la información y las comunicaciones, sobre todo cuando se trate de cuestiones de género relacionadas con la ciberdelincuencia, a fin de promover la igualdad de género y el empoderamiento de las mujeres en y fuera de Internet.

b) Se debería hacer frente a los delitos cibernéticos y evitar y combatir la violencia contra las mujeres y los niños.

China

[Original: chino]
[5 de noviembre de 2021]

China acoge con beneplácito la invitación remitida por la Presidencia del Comité Especial de las Naciones Unidas encargado de Elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos a los Estados Miembros para que presentasen su opinión sobre el ámbito de aplicación, los objetivos y la estructura (los elementos) de la convención. De conformidad con lo dispuesto en la resolución 75/282 de la Asamblea General, el Comité Especial deberá presentar un proyecto de convención a la Asamblea General en su septuagésimo octavo período de sesiones. China espera con interés que tengan lugar conversaciones constructivas bajo la dirección de la Presidencia para llegar, cumpliendo el calendario, a una nueva convención que sea universal, tenga autoridad y resulte aceptable para todas las partes, a fin de ofrecer un marco jurídico que fortalezca la cooperación contra la ciberdelincuencia a escala mundial.

Hasta ahora los Estados Miembros se han valido de los mecanismos pertinentes de las Naciones Unidas para mantener debates en profundidad sobre la lucha contra la ciberdelincuencia y han convenido algunas conclusiones y recomendaciones. Además, un Estado Miembro ha presentado un proyecto de convención general que constituye una referencia importante para la negociación de la convención. China acoge con agrado la labor de la Presidencia de alentar a los Estados Miembros a que presenten su opinión y proyectos de propuestas y respalda los preparativos de la Presidencia encaminados a elaborar un borrador preliminar de la convención a partir de las comunicaciones de los Estados Miembros con miras a empezar a negociar el texto de la convención lo antes posible.

Con ánimo de apoyar la labor de la Presidencia y del Comité Especial, China expone a continuación su opinión sobre el ámbito de aplicación, los objetivos y la estructura (los elementos) de la convención y está dispuesta a participar en negociaciones constructivas con todas las partes.

I. Objetivos

a) Promover y fortalecer las medidas encaminadas a combatir y prevenir con más eficiencia y eficacia la utilización de las tecnologías de la información y las comunicaciones (TIC) con fines delictivos, con miras a hacer realidad la visión de un futuro compartido en la comunidad del ciberespacio.

b) Promover, facilitar y apoyar la cooperación internacional para prevenir y combatir la utilización de las TIC con fines delictivos, teniendo en cuenta las particularidades de esas tecnologías y la necesidad de combatir las actividades delictivas conexas. Esa cooperación internacional puede consistir, entre otras cosas, en coordinar, entre los Estados Miembros, las normas por las que se tipifiquen delitos; en proporcionar orientaciones para solucionar los conflictos de jurisdicción y en formular arreglos institucionales más específicos en materia de cooperación en lo que respecta a la aplicación de la ley, la asistencia jurídica, la extradición y la recuperación de activos.

c) Fortalecer la cooperación en materia de creación de capacidad y asistencia técnica y promover el intercambio de información al respecto en consonancia con las necesidades más amplias de cooperación internacional y con los intereses de los países en desarrollo.

II. Ámbito de aplicación

La convención debería aplicarse a la prevención, la investigación y el enjuiciamiento de la utilización de las TIC con fines delictivos por personas físicas o grupos de delincuentes, así como al bloqueo, el embargo preventivo, la incautación, el decomiso y la restitución del producto de los delitos relacionados con las TIC.

La utilización de las TIC con fines delictivos debería aplicarse, como mínimo, a los delitos que atenten contra datos, sistemas e instalaciones de TIC, así como a los delitos cometidos valiéndose de las TIC.

III. Estructura (elementos)

La convención podría dividirse en siete capítulos: disposiciones generales; prevención; tipificación y aplicación de la ley; cooperación internacional; asistencia técnica e intercambio de información; mecanismo de aplicación; y disposiciones finales.

A continuación figura una propuesta preliminar de los elementos que podrían figurar en cada capítulo.

1. Disposiciones generales

Además de los objetivos y del ámbito de aplicación, debería incluirse el contenido siguiente:

a) *Protección de la soberanía*. El principio de la igualdad soberana de todos los Estados consagrado en la Carta de las Naciones Unidas es la norma básica de las relaciones internacionales contemporáneas. La aplicación del principio de soberanía al ciberespacio también goza de un amplio apoyo por parte de los Estados Miembros. En la convención se debería estipular que los Estados partes deberán cumplir las obligaciones dimanantes de la convención respetando los principios de la igualdad soberana, de la integridad territorial y de la no injerencia en los asuntos internos de los otros Estados.

b) *Terminología*. Se deberían dar definiciones de los términos y las expresiones clave que se utilicen en la convención, por ejemplo, pruebas electrónicas, información personal, infraestructura de información esencial, almacenamiento en la nube, proveedor de servicios en red, programa malicioso, botnet, información dañina y ciberataque.

2. Prevención

Se debería resaltar la importancia de prevenir la utilización de las TIC con fines delictivos. El principio básico debería ser “la prevención es lo primero, al tiempo que se combate la delincuencia”. Se deberían exponer con claridad las responsabilidades de los Gobiernos y del sector privado en la prevención del delito, y los Gobiernos deberían formular medidas específicas de prevención del delito, alentando al mismo tiempo la

participación de la sociedad y la cooperación entre los sectores público y privado. Deberían incluirse los siguientes elementos:

a) Se debería alentar a los Estados Miembros a que designasen organismos especializados que formulasen políticas en materia de prevención de la utilización de las TIC con fines delictivos y llevasen a cabo evaluaciones con regularidad. Los Estados Miembros deberían establecer medidas para proteger la seguridad de la infraestructura de información esencial así como establecer sistemas de protección de la seguridad para distintos niveles de red. Se deberían adoptar distintas tecnologías de seguridad de la información y medidas de gestión para distintas instalaciones de red a fin de proteger la infraestructura de información esencial contra posibles ataques de delincuentes o grupos delictivos. Se debería aumentar la capacidad de prevención del delito de los departamentos gubernamentales pertinentes.

b) Los Estados Miembros deberían promulgar leyes nacionales que estableciesen claramente las responsabilidades del sector privado, incluidos los proveedores de servicios en red, en lo que respecta a prevenir la utilización de las TIC con fines delictivos, o mejorar las leyes nacionales existentes. Esas responsabilidades deberían abarcar, entre otras cosas, las precauciones de seguridad (por ejemplo, formular planes de emergencia para casos de incidencias que afecten a la seguridad de una red, hacer frente de manera oportuna a aspectos vulnerables de los sistemas y del equipo informático, a virus informáticos, a ataques contra una red o a intrusiones en una red y adoptar medidas en tiempo real cuando se descubra que los servicios de un proveedor podrían estar utilizándose para realizar actividades delictivas) y la retención de la información de registro (los Gobiernos deberían especificar el contenido estándar y el período durante el que se deberá retener la información de registro). Al determinar las responsabilidades de los proveedores de servicios en red, se deberían concertar arreglos adaptados a cada nivel y conformes al principio de proporcionalidad, teniendo muy presentes las diferencias que existen en cuanto a capacidad entre los proveedores de servicios en red de distintos tamaños.

c) Se debería alentar a los Gobiernos, al sector privado y a las comunidades a participar en distintas modalidades de cooperación público-privada. En particular, se deberían redoblar los esfuerzos encaminados a sensibilizar al público en materia de prevención del delito.

3. Tipificación y aplicación de la ley

Cada vez son más los delincuentes y los grupos delictivos que hacen un uso indebido de las TIC para cometer delitos, lo que está dando lugar a una “cadena de producción” oscura especializada en el desarrollo de TIC con fines delictivos y a transacciones en las que se utilizan esas tecnologías y datos conexos. La convención debería ofrecer un marco más flexible, orientado hacia el futuro, para coordinar la tipificación de conductas, responder a las necesidades relacionadas con el desarrollo actual y ulterior de las TIC y atender la necesidad de combatir la delincuencia. En la convención también se deberían prever los mecanismos pertinentes en relación con la jurisdicción, la aplicación de la ley y las pruebas electrónicas, a saber:

a) Se debería solicitar a los Estados Miembros que tipificasen como delitos la intrusión en instalaciones, sistemas, datos o infraestructura de información esencial que guarden relación con las TIC, así como su destrucción. Esto podría comprender el acceso ilícito a sistemas de información computarizada, la injerencia ilegal en sistemas de información computarizada, la adquisición ilegal de datos informáticos, la injerencia ilegal en datos informáticos y la intrusión en la infraestructura de información esencial, entre otros actos.

b) En la convención se podrían enumerar, según proceda, las actividades delictivas que se perpetran utilizando TIC y que gozan de un amplio reconocimiento en la comunidad internacional, como la ciberextorsión, el fraude cibernético, la pornografía cibernética

(sobre todo la utilización de niños en la pornografía), la utilización de las TIC para infringir derechos de autor y otros derechos conexos y la utilización de Internet para cometer actos de terrorismo o incitar a cometerlos o para difundir información dañina, entre otros actos.

c) En cuanto a otros delitos que se cometan utilizando las TIC, se debería poner de relieve que los Estados Miembros pueden combatir y prevenir otros delitos pertinentes que no figuren en la convención, y que pueden colaborar en el plano internacional en consonancia con la convención, con otros tratados internacionales y con la legislación nacional pertinente de los Estados Miembros.

d) En vista de la creciente "industrialización" de los delitos que se cometen utilizando las TIC, la señalada "cadena de producción" oscura se debería incluir entre las conductas tipificadas, junto con medidas más estrictas para reprimir la instigación o preparación de esos actos delictivos, entre ellos, el desarrollo, la venta o la difusión de TIC o de datos con fines delictivos.

e) Respecto de la expresión "pruebas electrónicas", se deberían fijar las normas para definir qué constituyen pruebas electrónicas en los procesos judiciales penales, en particular, cómo establecer la autenticidad de esas pruebas, su integridad, legitimidad y pertinencia.

f) Se podría solicitar a los Estados Miembros que formulasen leyes nacionales, o mejorasen las existentes, con miras a exponer con claridad las obligaciones del sector privado, por ejemplo, la obligación de los proveedores de servicios en red de cooperar con los organismos encargados de hacer cumplir la ley en lo que respecta a vigilar, investigar y combatir los delitos. Otros ejemplos de obligaciones que se deberían incluir son la retención de la información de registro, la conservación de los datos y las pruebas cumpliendo unas normas unificadas en cuanto a contenido y plazos y la cooperación con los organismos encargados de hacer cumplir la ley. Al determinar las obligaciones de los proveedores de servicios en red, se deberían concertar arreglos adaptados a cada nivel y conformes al principio de proporcionalidad, teniendo muy presentes las diferencias que existen en cuanto a capacidad entre los proveedores de servicios en red de distintos tamaños. En el caso de que un proveedor de servicios en red incumpliera sus obligaciones, los Estados Miembros deberían imponerle sanciones administrativas y penales eficaces con arreglo a su derecho interno.

g) Se deberían proporcionar orientaciones para resolver los conflictos de jurisdicción. Dadas las particularidades del ciberespacio y de las TIC, se deberían fijar normas para determinar la jurisdicción y evitar esos conflictos. La determinación de la jurisdicción debería fundamentarse en la existencia de un vínculo "verdadero y suficiente" con la actividad delictiva de la que se trate, dando prioridad al lugar en el que se produjeran las consecuencias de la actividad delictiva, al lugar en el que se cometiera el delito y al lugar en el que se encontrara la persona o el grupo que lo cometió. Si fuera difícil formular esas normas, se deberían establecer normas de exclusión: por ejemplo, un Estado no debería poder reclamar para sí jurisdicción sobre una causa relacionada con las TIC argumentando meramente que los datos pasaron por ese Estado. En caso de que se produjera un conflicto de jurisdicción, esta se debería determinar mediante consultas con arreglo a los principios del *forum conveniens* y la facilitación de la recuperación de activos.

h) También se deberían incluir disposiciones sobre la asistencia para cometer un delito o la incitación a este, la tentativa de delito, los delitos cometidos por una persona jurídica, etcétera.

4. Cooperación internacional

La utilización de las TIC con fines delictivos tiene un fuerte carácter transnacional y supone un desafío compartido para toda la comunidad internacional. Además, en el marco jurídico internacional vigente, el anonimato y el alto grado de inteligencia que entrañan las

actividades delictivas, sumados a la inestabilidad y al carácter perecedero de las pruebas electrónicas, plantean dificultades notables para el funcionamiento de mecanismos de cooperación internacional como la asistencia judicial recíproca. Los Estados Miembros deberían colaborar entre sí tanto como fuera posible para combatir y prevenir la utilización de las TIC con fines delictivos, y al hacerlo deberían respetar el principio de reciprocidad, estudiar seriamente la posibilidad de adoptar medidas innovadoras en el plano institucional y proponer mecanismos nuevos que permitan que la cooperación internacional esté dirigida a cuestiones más específicas.

a) La obtención transfronteriza de pruebas electrónicas es necesaria para combatir la utilización de las TIC con fines delictivos, pero los Estados Miembros deberían respetar la soberanía del Estado en el que se hallasen ubicadas las pruebas. Además, para la obtención transfronteriza de pruebas electrónicas, los Estados Miembros deberían respetar las garantías procesales y los derechos legítimos de las personas y las entidades y no deberían emplear medios de investigación técnicos que fueran invasivos ni destructivos. Los Estados no deberían obtener datos alojados por empresas o individuos en otros Estados de manera directa ni valiéndose de medios técnicos que sorteasen las medidas de protección de una red si esos medios vulnerasen el ordenamiento jurídico de ese otro Estado. Los Estados Miembros deberían estudiar nuevos arreglos institucionales para obtener pruebas electrónicas de otros Estados, por ejemplo, la autenticación de pruebas electrónicas y la obtención de pruebas en imagen (o sonido) sobre la base de la confianza mutua. En relación con esos arreglos, se debería hacer lo posible por ofrecer orientaciones unificadas y fehacientes para la obtención transfronteriza de pruebas electrónicas, conciliando al mismo tiempo dos objetivos distintos entre sí como son el respeto de la soberanía nacional y la lucha contra el delito.

b) Los Estados Miembros deberían formular mecanismos que hicieran posible cooperar rápidamente en lo que respecta a aplicación de la ley. Podrían designar organismos concretos que cumpliesen funciones de enlace y, de ese modo, permitiesen un rápido intercambio de pistas sobre los delitos, la prestación de asesoramiento técnico y otras formas de cooperación en materia de aplicación de la ley cuando surgiesen necesidades especiales.

c) A fin de aumentar la eficiencia de la asistencia judicial recíproca en las causas penales, los Estados Miembros podrían establecer un mecanismo rápido de enlace y respuesta entre las autoridades competentes que permitiera la comunicación en tiempo real cuando esta fuera necesaria. La transmisión de documentos legales y pruebas electrónicas, como parte de la obtención transfronteriza de pruebas, se podría llevar a cabo en línea por medios técnicos (por ejemplo, con las firmas electrónicas) en el marco de los sistemas transfronterizos nacionales para la gestión de la seguridad en la transmisión de datos. También podrían elaborarse disposiciones sobre asistencia judicial recíproca para casos de emergencia, por ejemplo, la conservación urgente de pruebas electrónicas, la revelación rápida de información tras haberse tomado medidas para la conservación de datos, etcétera.

d) Teniendo en cuenta que el sector privado, incluidos los proveedores de servicios en red, tiene la obligación —que se deberá definir en la legislación nacional— de cooperar con los organismos encargados de hacer cumplir la ley en lo que respecta a vigilar, detectar y combatir las actividades delictivas, los Estados Miembros, especialmente los que cuentan con recursos en red avanzados, deberían reforzar la cooperación internacional. Si las instalaciones, los sistemas o las redes de TIC que son propiedad de un proveedor de servicios en red del Estado A son utilizados por un sospechoso situado en otro Estado para cometer un delito, entonces, siempre que el Estado A también hubiera tipificado como delito el acto del que se tratase, el Estado A, por iniciativa propia o a instancia del otro Estado, debería exigir al mencionado proveedor de servicios en red que aplicase las medidas técnicas o de otra índole que fuesen necesarias para responder de manera eficaz frente al acto delictivo.

e) Se deberían fortalecer las medidas que fueran pertinentes para impedir y bloquear la transferencia internacional del producto de delitos y aumentar la cooperación internacional en lo que respecta a la recuperación de activos. Los Estados Miembros deberían atenerse al principio de la recuperación rápida y eficaz de activos y no deberían fijar ninguna condición previa para esa recuperación que no fuera el cumplimiento del procedimiento judicial de que se tratara.

5. Asistencia técnica e intercambio de información

Es esencial proporcionar asistencia técnica a los países en desarrollo y fortalecer el intercambio de información con ellos para combatir y prevenir eficazmente la utilización de las TIC con fines delictivos.

a) La asistencia técnica que se preste a los países en desarrollo debería incluir:

i) capacitación para los funcionarios judiciales y de los organismos encargados de hacer cumplir la ley;

ii) capacitación para equipos de profesionales que cuenten con conocimientos especializados tanto jurídicos como técnicos;

iii) creación de capacidad en la esfera de la obtención de pruebas electrónicas;

iv) suministro de equipo y tecnología pertinentes, según proceda, para ayudar a los países en desarrollo a reforzar su capacidad para combatir la delincuencia;

v) fomento de la participación de organizaciones internacionales, como la Oficina de las Naciones Unidas contra la Droga y el Delito, el sector privado, expertos y miembros del sector académico, en las actividades de asistencia técnica y creación de capacidad.

b) Se debería alentar a los Estados Miembros a intercambiar experiencias sobre la formulación y la aplicación de las leyes y políticas, así como a intercambiar datos relacionados con la represión y la prevención del delito y de las tendencias conexas.

6. Mecanismo de aplicación

Con el fin de promover la aplicación de la convención, se debería establecer una conferencia de los Estados partes y grupos de expertos o grupos de trabajo pertinentes, por ejemplo, un grupo de trabajo sobre asistencia técnica y otro sobre cooperación internacional. Las reuniones de esos grupos podrían servir también como foro para que los Estados partes intercambiasen experiencias y promoviesen la cooperación.

7. Disposiciones finales

Sin comentarios por el momento.

Colombia

[Original: español]
[5 de noviembre de 2021]

Habida cuenta de la aprobación de la resolución 74/247 de la Asamblea General, por medio de la cual se estableció un comité intergubernamental especial de expertos de composición abierta para elaborar una convención internacional integral sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones (TIC) con fines delictivos, y considerando la invitación de la Presidente del Comité Especial para que los Estados Miembros presenten posiciones nacionales sobre el alcance, los objetivos y la estructura que debería tener el futuro convenio sobre el delito cibernético, a continuación nos permitimos remitir los comentarios preliminares de Colombia:

Ámbito de aplicación

El nuevo convenio debería centrarse en la búsqueda de una herramienta de cooperación jurídica internacional para la prevención, la investigación, el juzgamiento y la sanción de los delitos cibernéticos por las autoridades nacionales y en lo relacionado con las evidencias electrónicas. Por lo tanto, se deben evitar discusiones que no se centren en el problema jurídico de la cibercriminalidad y la gestión de las evidencias electrónicas.

Deben evitarse discusiones sobre temas que puedan ser políticamente álgidos y que no se refieran directamente al núcleo del convenio a negociar.

Se considera fundamental que la nueva convención tenga en cuenta los marcos e instrumentos jurídicos internacionales existentes, entre los que se encuentran la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, la Convención de las Naciones Unidas contra la Corrupción y el Convenio sobre la Ciberdelincuencia (Convenio de Budapest), dado que la legislación nacional y las prácticas de la mayoría de los Estados están conformes o se sustentan en los acuerdos existentes, por lo cual los estándares futuros deben ser compatibles con estos. Asimismo, se debe garantizar que no se desarrollen normas que generen conflicto o riñan con otras obligaciones internacionales adoptadas por los Estados.

En ese sentido, el convenio debe tener un enfoque complementario, es decir, que la negociación debe considerar, en principio, el trabajo que la comunidad internacional ya viene realizando desde hace algunos años en la lucha contra el cibercrimen y no contradecir las diferentes obligaciones internacionales aplicables de los respectivos Estados. Por lo tanto, se deben aprovechar las potencialidades y los avances que la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional ha traído en materia dogmática y de herramientas de cooperación judicial.

Deben tenerse en cuenta los marcos multilateral, regional y bilateral actualmente vigentes en materia de asistencia judicial mutua a fin de evitar posibles conflictos normativos, complementar y utilizar los instrumentos internacionales ya existentes y no obstaculizar su efectiva aplicación. Así, debe recomendarse no solo la consideración exhaustiva de antecedentes multilaterales como la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y el Convenio sobre la Ciberdelincuencia, sino también los acuerdos bilaterales y regionales, como es el caso de la Convención Interamericana sobre Asistencia Mutua en Materia Penal.

Específicamente, debe tenerse en cuenta el Convenio sobre la Ciberdelincuencia, aprobado en 2001 en Budapest, ya que incluye conceptos ampliamente debatidos y una experiencia fáctica internacional de 20 años. Su no observación traería consigo el riesgo de entrar en un camino que contravenga los avances ya obtenidos en la lucha contra la cibercriminalidad.

Asimismo, el proceso debe considerar los resultados del trabajo del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético en el marco de las Naciones Unidas, y aprovechar el listado de conclusiones y recomendaciones preliminares sugeridas por los Estados Miembros durante las reuniones del Grupo de Expertos.

Resaltamos la importancia de que la elaboración de la nueva convención se realice de forma inclusiva y transparente y, hasta donde sea posible, se base en el consenso, como se llevaron a cabo los anteriores procesos de las Naciones Unidas para concertar la Convención contra la Delincuencia Organizada Transnacional y la Convención contra la Corrupción, para contribuir a prevenir futuras controversias en la materia.

Objetivo

El objetivo general de la convención debería ser la adopción de un marco de cooperación internacional en materia de justicia para la prevención, investigación y

persecución integral sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, la cibercriminalidad, y lo relacionado con las evidencias electrónicas.

Estructura

- Línea base de definiciones y conceptos tecnológicos estandarizados y con vocación de permanencia en el tiempo.
- Disposiciones sustantivas (tipos penales que deban ser adoptados en las legislaciones nacionales).

En tal sentido, la convención debería dar relevancia penal a un conjunto de conductas que afectan la información y los sistemas informáticos.

Parece razonable centrarse, por orden dogmático y metodológico, exclusivamente en los llamados delitos núcleo de la cibercriminalidad: delitos de acceso informático no autorizado a redes o sistemas informáticos a través del delito de acceso abusivo a un sistema informático; el espionaje informático, que asocia todas las conductas que vulneren la intimidad de personas naturales y jurídicas a través de la interceptación u obtención de datos, comunicaciones, archivos o bases de datos almacenados en sistemas informáticos o transmitidos a través de redes de comunicación, y que encierra los delitos de interceptación de datos informáticos, la violación de datos personales y la suplantación de sitios web para capturar datos personales; y el sabotaje informático, orientado a la obstaculización, daño, inutilización, supresión, interferencia o inutilización de sistemas informáticos, bases de datos o procesos de tratamiento, transferencia y transmisión de datos y que incluye los delitos de obstaculización ilegítima de un sistema informático o una red de telecomunicaciones.

De otra parte, se podrían incluir algunas conductas que, por cometerse a través de medios informáticos, tienen un fuerte impacto y alcance y su investigación encierra cierta complejidad, de manera que el instrumento sea lo suficientemente flexible como para servir de herramienta para combatir actividades ilegales conexas con otros delitos.

- Cláusula de doble incriminación: este mecanismo es importante con miras a lograr prestar la asistencia judicial recíproca independientemente de que el hecho que la origine no sea punible según la legislación del Estado requerido, garantizando así, entre otros aspectos, que los ciberdelincuentes no encuentren refugios seguros en algunos países por la ausencia de una legislación estándar común.
- Disposiciones procesales que permitan hacer efectiva la cooperación jurídica: en tal sentido, se considera imperativo intensificar la cooperación internacional en la investigación de los delitos cibernéticos, en especial frente a la gestión de pruebas digitales, cadena de custodia, conservación de datos y análisis forense. La transmisión y el almacenamiento de datos es un asunto que requiere atención urgente, así como la definición de mecanismos que permitan la comunicación y respuesta rápida entre las autoridades homólogas de los diferentes Estados, a través de canales digitales apropiados y seguros.
- Agravantes de las conductas que afectan el bien jurídico de la protección de la información y de los datos, como aquellas relacionadas con la captura masiva de datos personales, violación de los derechos humanos, o aquellas conductas que tengan como blanco infraestructuras críticas y servicios esenciales.
- Cooperación judicial internacional: facilitar, ampliar y agilizar las solicitudes de asistencia judicial mutua a través de canales digitales, con las seguridades que correspondan, y a través de formatos estándar.
- Definir mecanismos investigativos especializados en la recolección de evidencia digital, especialmente en lo relacionado con la evidencia que se encuentre almacenada en diferentes jurisdicciones.

- Es importante que los Estados Miembros acuerden mecanismos que garanticen un nivel adecuado de protección de los datos personales en el intercambio de información a través del instrumento internacional, no solo por la relevancia que en el entorno digital ha tomado la protección de los datos personales, sino también para evitar que las normas particulares de cada país puedan constituir eventualmente un obstáculo para el intercambio efectivo de información entre los Estados.
- Estímulo a la asistencia técnica y a la divulgación de conocimientos y buenas prácticas relacionados con la investigación, judicialización y sanción. Adicionalmente, para acortar la brecha digital, se considera fundamental que incluya el fortalecimiento de capacidades a instituciones encargadas de hacer cumplir la ley y otras autoridades de justicia nacionales, especialmente en lo referente a los programas de educación y entrenamiento como forma de prevención.
- Impulsar, a través de escuelas de capacitación regionales, la cooperación técnica. Dada la complejidad y la especificidad en la investigación de crímenes cometidos a través de medios informáticos, que no permiten investigar eficazmente, es necesario brindar capacitación especializada a los fiscales e investigadores de una manera organizada y continua, estableciendo previamente planes de trabajo con resultados esperados.
- Se resalta que la promoción de la cooperación sólida y basada en la confianza entre los sectores público y privado en el ámbito de la ciberdelincuencia es un tema de la mayor importancia, por lo cual resulta fundamental tener una posición consistente en el tema, y que se facilite la obtención de evidencia digital por parte de actores en el entorno digital, incluyendo a las empresas prestadoras de servicios de Internet (ISP) y comunicaciones.
- Promover y facilitar el acceso de autoridades a plataformas colaborativas para el fortalecimiento de capacidades y el intercambio de información, así como a herramientas de análisis y contexto, para las investigaciones en esta materia.
- Disposiciones que faciliten el acceso a información expedita en casos de emergencia.
- Finalmente, se sugiere incluir la creación de una red de puntos de contacto con atención permanente (24 horas/7 días de la semana) para la atención de las solicitudes de cooperación jurídica internacional en la materia, que adicionalmente podría complementarse con una red de contactos para: a) potenciar el intercambio de conocimientos y experiencias en materia de ciberdelitos y delitos conexos; b) crear y divulgar las buenas prácticas y, c) optimizar y agilizar la cooperación judicial internacional entre los distintos países.

Egipto

[Original: árabe]
[28 de octubre de 2021]

La República Árabe de Egipto, deseosa de contribuir positivamente a los esfuerzos internacionales encaminados a formular una convención integral de las Naciones Unidas sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, y cumpliendo los compromisos que ha contraído en virtud de tratados y convenciones nacionales, regionales e internacionales relativos a los derechos humanos y a la lucha contra la delincuencia transnacional, ha preparado la presente comunicación en la que propone elementos preliminares para su integración en el cuerpo de la mencionada convención, con la esperanza de alcanzar los objetivos deseados mediante el fortalecimiento de la cooperación internacional y la formulación de una política común en materia de delincuencia destinada a luchar contra todos los delitos relacionados con las tecnologías de la información y las comunicaciones (TIC) a fin de sortear los peligros que

plantean esos delitos para la seguridad y los intereses de los Estados y la seguridad de sus comunidades y ciudadanos.

I. Objetivos

La convención debería tener por finalidad reforzar la cooperación entre los Estados Miembros de las Naciones Unidas en la lucha contra la utilización de las TIC con fines delictivos, a fin de prevenir cualquier acto que amenace la integridad y la confidencialidad de esas tecnologías, tipificar como delito su uso indebido con fines ilícitos, facilitar los medios de investigación y enjuiciar a los autores. La convención también debería prever la eliminación de las consecuencias de los delitos relacionados con la utilización de las TIC, como la suspensión de las transacciones vinculadas a activos obtenidos de resultas de la comisión de cualquier acto ilegal mencionado en la convención, y el decomiso y la restitución del producto de dichos delitos, otorgando poderes suficientes para contrarrestar eficazmente los delitos relacionados con las TIC mediante el establecimiento de acuerdos de cooperación internacional destinados a facilitar la detección, la investigación y el enjuiciamiento de dichos delitos así como la extradición.

II. Ámbito de aplicación

1. Salvo que se disponga lo contrario, la convención debería aplicarse a la prevención de los delitos que se contemplen en sus disposiciones.

2. Cada Estado parte debería adoptar todas las medidas necesarias para establecer su jurisdicción respecto de los delitos y otros actos ilícitos tipificados como tales en la convención, cuando el delito:

a) se cometa en su territorio; o

b) se cometa a bordo de un buque que enarbole el pabellón de ese Estado parte o a bordo de una aeronave registrada conforme a la legislación de ese Estado parte en ese momento; o

c) sea de carácter transnacional y en su comisión participe un grupo delictivo organizado. Se debería considerar que un delito es de carácter transnacional si se ha cometido: i) en más de un país; ii) en un país, pero ha sido parcialmente preparado, planificado, dirigido o supervisado desde otro país; iii) en un país, por obra de un grupo delictivo organizado que realiza actividades delictivas en más de un país; iv) en un país, pero entraña graves consecuencias en otro.

3. A los efectos de la aplicación de la convención, no debería ser necesario que los delitos u otros actos ilícitos mencionados en la convención ocasionen daños materiales, salvo que se disponga lo contrario.

4. Los Estados partes deberían considerar la posibilidad de restringir la formulación de reservas para propiciar una amplia aplicación de las medidas antes mencionadas.

III. Protección de la soberanía

1. Cada Estado parte debería cumplir, de conformidad con su legislación nacional y sus principios constitucionales, sus obligaciones dimanadas de la aplicación de la convención en consonancia con los principios de igualdad soberana de los Estados y de no injerencia en los asuntos internos de otros Estados.

2. La convención no debería facultar a las autoridades competentes de un Estado parte para ejercer en el territorio de otro Estado parte la jurisdicción y las funciones que el derecho interno de ese Estado reserve exclusivamente a sus autoridades.

IV. Delitos que se propone incluir en la convención

1. Cada Estado parte debería adoptar las medidas legislativas y de otra índole que sean necesarias para prevenir la comisión de los delitos mencionados en la convención o cualquier otro delito relacionado con la utilización de las TIC, incluidos el bloqueo y la eliminación de contenidos vinculados a dichos delitos; detectar delitos; enjuiciar a los autores; extraditar a los delincuentes y facilitar los procedimientos de cooperación internacional y reunión de pruebas.

2. Cada Estado parte debería adoptar asimismo las medidas legislativas y de otra índole que sean necesarias para tipificar como delito los siguientes actos:

Artículo 1. La utilización ilícita de servicios y tecnologías de la información y las comunicaciones, incluida la obtención de un beneficio ilícito, o la incitación a otros a que obtengan un beneficio ilícito, desde servicios de telecomunicaciones o canales de audio o vídeo transmitidos a través de las redes de información o de un dispositivo de tecnologías de la información y las comunicaciones.

Artículo 2. El acceso ilícito o el acto de rebasar los límites del derecho de acceso, incluidos:

1. El uso de una autorización especial concedida para acceder a un sitio web, una cuenta privada o un sistema de información de forma que se excedan los límites de esa autorización especial en cuanto a la duración del acceso o nivel de acceso.

2. El acceso ilícito a la totalidad o una parte de un sistema de tecnología de la información o la comunicación con el conjunto o parte de ese sistema y la continuación de dicho acceso o comunicación.

3. La pena por este delito debería incrementarse si dicho acceso o comunicación diera lugar a lo siguiente:

a) la supresión, la modificación, la distorsión, la reproducción, la transferencia o la destrucción de datos guardados, de dispositivos y sistemas electrónicos o de redes de comunicación, o a un perjuicio causado a usuarios y beneficiarios;

b) acceso a información gubernamental confidencial.

Artículo 3. El ataque al diseño de un sitio web mediante la destrucción, la disrupción, la ralentización, la distorsión, la ocultación o la modificación ilícitas del diseño del sitio web de una empresa, institución, instalación o persona física.

Artículo 4. La interceptación deliberada e ilícita de un flujo de datos por cualquier medio técnico o mediante la interrupción de la transmisión o recepción de datos de la tecnología de la información.

Artículo 5. La violación de la integridad de los datos mediante la destrucción, la supresión, la obstrucción, la modificación o el bloqueo de datos de la tecnología de la información de forma intencionada e ilegal.

Artículo 6. La utilización indebida de la tecnología de la información para la producción, la venta, la compra, la importación, la distribución, el suministro o la posesión de herramientas o programas informáticos diseñados o adaptados, contraseñas o información similar mediante las cuales se pueda acceder a un sistema de información con la intención de utilizarlo para cometer uno de los delitos mencionados en la convención, o la creación de programas informáticos maliciosos destinados a destruir, bloquear, modificar, reproducir o difundir información digital, o la neutralización de los elementos de seguridad, salvo con fines de investigación lícita.

Artículo 7. La falsificación mediante el uso de la tecnología de la información para alterar la veracidad de la información de manera perjudicial con la intención de utilizar la información alterada como información válida.

Artículo 8. El fraude, en perjuicio de beneficiarios y usuarios, de manera intencionada e ilegal, cometido a fin de obtener de manera ilícita derechos y beneficios para el autor o para otras personas, entre otras cosas a través de delitos electrónicos fraudulentos relacionados con monedas virtuales (digitales o encriptadas).

Artículo 9. La amenaza o extorsión utilizando las TIC o cualquier otro medio tecnológico para amenazar o chantajear a una persona a fin de que cometa o se abstenga de cometer un acto.

Artículo 10. Pornografía, en la que:

1. las TIC se utilicen para producir, exhibir, distribuir, proporcionar, publicar, comprar, vender o importar materiales pornográficos con fines obscenos;

2. las TIC se utilizan para producir, exhibir, distribuir, proporcionar, publicar, comprar, vender o importar materiales de pornografía infantil o de menores, así como para poseer dichos materiales o materiales que representen a niños o menores de forma indecente en las TIC o en cualquier medio de almacenamiento de TIC.

Artículo 11. Otros delitos relacionados con la pornografía, como la explotación o el acoso sexuales, especialmente de mujeres, niños o menores.

Artículo 12. La incitación o coacción al suicidio, en particular dirigidas a menores para que se suiciden, mediante presiones psicológicas o de otra índole en las redes de información y comunicaciones, entre ellas Internet, ya sea mediante la interacción directa o mediante tecnologías populares o juegos electrónicos.

Artículo 13. La utilización de las TIC para involucrar a menores en la comisión de actos ilícitos que pongan en peligro su vida o su salud física o mental.

Artículo 14. La utilización de las TIC para violar la privacidad, incluso mediante la creación de un correo electrónico, un sitio web o una cuenta privada y su atribución falsa a una persona física o jurídica.

Artículo 15. La utilización de la tecnología de la información para cometer delitos relacionados con el terrorismo, entre otros los siguientes:

1. la difusión de las ideas y los principios de grupos terroristas o la justificación del terrorismo;

2. la financiación de operaciones terroristas o el adiestramiento para dichas operaciones, la facilitación de la comunicación entre organizaciones terroristas o el suministro de apoyo logístico a personas que lleven a cabo operaciones terroristas;

3. la difusión de métodos de fabricación de explosivos, especialmente para su utilización en operaciones terroristas;

4. la propagación del fanatismo, la sedición, el odio o el racismo.

5. Los Estados partes deberían adoptar las medidas necesarias para prohibir la difusión de esos contenidos en los medios de TIC, como el bloqueo y la eliminación de los contenidos relacionados con esos delitos.

Artículo 16. Delitos financieros, como el blanqueo de dinero, y que abarquen:

1. la utilización de las TIC para cometer delitos financieros o hacer un uso indebido de monedas virtuales (digitales o encriptadas);

2. la realización de operaciones de blanqueo de dinero, o la solicitud de ayuda o la difusión de métodos para llevarlas a cabo.

Artículo 17. La utilización ilícita de instrumentos de pago electrónicos, incluidas:

1. la falsificación, fabricación o creación por cualquier medio de cualquier dispositivo o material que facilite la falsificación o imitación de cualquier instrumento de pago electrónico;

2. la apropiación de los datos de un instrumento de pago, la utilización de esos datos, su entrega a otros o la instigación a obtener dichos datos para otros;

3. la utilización de una red de información o una tecnología de la información para obtener un acceso no autorizado al código o a los datos de un instrumento de pago;

4. la aceptación deliberada de un instrumento de pago falsificado.

Artículo 18. Los delitos relacionados con la delincuencia organizada o la delincuencia transnacional cometidos por medio de la tecnología de la información, incluidos:

1. la comercialización o el tráfico ilícito de estupefacientes o sustancias sicotrópicas;

2. la distribución ilícita de medicamentos o productos sanitarios falsificados;

3. el tráfico ilícito de migrantes;

4. la trata de personas;

5. el tráfico de órganos humanos;

6. el comercio ilícito de armas;

7. el tráfico ilícito de bienes culturales.

Artículo 19. Los delitos relacionados con la infracción de los derechos de autor y derechos conexos, incluida la violación de los derechos de autor y derechos conexos definida en la legislación del Estado parte, si el acto se comete intencionadamente.

Artículo 20. El acceso no autorizado a la infraestructura de información crítica, incluidas:

1. la creación, distribución o utilización de programas informáticos u otra información digital para proporcionar acceso no autorizado a una infraestructura de información crítica, incluidos la destrucción, el bloqueo, la modificación o la reproducción de la información contenida en ella o la neutralización de sus elementos de seguridad;

2. la violación de las normas de funcionamiento establecidas para los soportes destinados al almacenamiento, el tratamiento o la transferencia de información digital protegida contenida en infraestructuras de información o sistemas de información críticos, o de información protegida en virtud de la legislación nacional del Estado parte, y de las redes de comunicación pertenecientes a infraestructuras de información críticas, o la violación de las normas de acceso a ellas, si dicha violación daña las infraestructuras de información críticas.

Artículo 21. La incitación a realizar actividades subversivas o armadas u otros delitos, incluidos los llamamientos emitidos a través de las TIC a la realización de actividades subversivas o armadas dirigidas contra el Gobierno de otro Estado que socavarían la seguridad pública y la estabilidad, o los llamamientos a la comisión de delitos punibles con penas de prisión no inferiores a un año.

Artículo 22. Los delitos relacionados con el extremismo, incluida la distribución de materiales que propugnen o justifiquen actos ilícitos basados en motivos políticos, ideológicos, sociales o étnicos o que inciten al odio por razones étnicas o religiosas o a la enemistad en general; o la facilitación del acceso a dichos materiales.

Artículo 23. La tentativa de cometer cualquiera de los delitos contemplados en la convención, incluida la participación en calidad de cómplice en la organización o dirección de otras personas para cometer esos delitos.

Artículo 24. Otros actos ilícitos.

La convención no debería ser obstáculo para que un Estado parte tipificara como delito cualquier otro acto ilícito cometido intencionadamente mediante la utilización de las TIC que causara un daño sustancial.

V. Responsabilidad jurídica, procedimientos penales, aplicación de la ley y asistencia judicial internacional

Artículo 1. Responsabilidad de las personas jurídicas

Con sujeción a su legislación nacional, cada Estado parte debería determinar la responsabilidad penal de una persona jurídica por los delitos cometidos por sus representantes en su nombre o en su beneficio, sin perjuicio de que se impongan penas a una persona física, por ejemplo a un administrador de sitio, que haya cometido el delito.

Artículo 2. Responsabilidad de los proveedores de servicios o administradores de sitios

Sin perjuicio de lo dispuesto en la convención, los proveedores de servicios o administradores de sitios y sus subordinados deberían cumplir las siguientes obligaciones, cuya violación debería ser tipificada como delito:

1. Guardar y almacenar el registro del sistema de información o el registro de cualquier tecnología de la información durante un período que se ha de determinar. Los datos que deben conservarse y almacenarse deberían incluir:

a) los datos que permitan identificar al usuario del servicio;

b) los datos relacionados con el contenido del sistema de información del cliente siempre que estén bajo el control del proveedor de servicios;

c) los datos relacionados con el tráfico de comunicaciones;

d) los datos relativos a los equipos periféricos de comunicación;

e) cualquier otro dato especificado por el Estado con miras a la aplicación de la convención.

2. Mantener la confidencialidad de los datos guardados y almacenados y abstenerse de divulgarlos sin orden motivada de una autoridad competente, incluidos los datos personales de cualquiera de los usuarios del servicio o cualquier dato o información relacionados con los sitios o las cuentas privadas a los que acceden dichos usuarios o las personas o entidades con las que estos se comunican.

3. Asegurar los datos y la información de manera que se mantenga su confidencialidad y se los proteja de la violación de datos e información y daños.

4. El proveedor de servicios o administrador del sitio debería proporcionar a los usuarios del servicio y a cualquier autoridad competente los siguientes datos e información, en una forma que propicie que su acceso a ellos sea fácil, directo y continuado:

a) el nombre y la dirección del proveedor de servicios;

b) la información de contacto del proveedor de servicios, incluida la dirección de correo electrónico;

c) los datos de la licencia para identificar al proveedor de servicios y a la autoridad competente que lo supervisa.

5. El proveedor de servicios o el administrador del sitio, previa solicitud de las autoridades competentes especificadas por el Estado, debería proporcionar toda la capacidad técnica necesaria para que las autoridades competentes puedan ejercer sus facultades.

Artículo 3. Procedimientos penales

1. Cada Estado parte debería adoptar las medidas legislativas y de otra índole necesarias para establecer las facultades y los procedimientos destinados a prevenir, reconocer, detectar e investigar delitos y otros actos ilícitos y entablar acciones judiciales al respecto.

2. Cada Estado parte debería aplicar las facultades y los procedimientos antes mencionados en relación con:

a) actos delictivos y otros actos ilícitos establecidos en la convención;

b) otros delitos u otros actos ilícitos cometidos por medio de las TIC;

c) la recopilación electrónica de pruebas de delitos.

3. Entre los procedimientos penales deberían figurar:

a) el aseguramiento expedito de los datos almacenados mediante tecnologías de la información, incluidos los parámetros técnicos del tráfico que hayan sido almacenados mediante esas tecnologías, especialmente si se cree que dicha información puede ser objeto de pérdida o modificación, ordenando a la persona interesada que preserve la integridad de la información que esté en su poder o bajo su control para permitir a las autoridades competentes efectuar búsquedas e investigaciones, manteniendo la confidencialidad de cualquier medida adoptada al respecto;

b) el aseguramiento expedito y la divulgación parcial de los parámetros técnicos del tráfico, independientemente de que uno o varios proveedores de servicios hayan transmitido la información, y la garantía de la pronta divulgación por las autoridades competentes de una cantidad justa de información que permita al Estado parte identificar al proveedor de servicios y la vía por la cual se transmitió la información;

c) la emisión de órdenes de proporcionar información que esté en poder de una persona en el territorio de un Estado parte y almacenada en una tecnología de la información o en un medio de almacenamiento, o en poder de un proveedor de servicios que preste sus servicios en el territorio o bajo el control del Estado parte;

d) la inspección de la información almacenada en un soporte de tecnología de la información o en un medio de almacenamiento, o el acceso a esa información;

e) el control, la reproducción y el aseguramiento de la información almacenada para llevar a cabo los procedimientos de búsqueda de información y acceso a la misma;

f) la obtención en tiempo real de los parámetros técnicos del tráfico y la obligación impuesta al proveedor de servicios dentro de la jurisdicción de reunir y registrar la información y de mantener su confidencialidad;

g) la interceptación del contenido de la información para que las autoridades competentes puedan reunir y registrar, por medios técnicos, la información transmitida en tiempo real mediante las TIC;

h) Cada Estado parte debería adoptar las medidas legislativas y de otra índole necesarias para que sus autoridades competentes puedan detener la transmisión y difusión de cualquier contenido que constituya un delito en virtud de la convención.

4. Aceptación de pruebas digitales

Las pruebas digitales derivadas o extraídas de dispositivos, equipos, medios electrónicos, sistemas de información, programas informáticos o cualquier medio de las TIC deberían tener el valor y la fuerza probatoria de las pruebas forenses materiales en las pruebas penales cuando dichas pruebas digitales cumplan las condiciones técnicas exigidas por las leyes de los Estados partes.

Artículo 4. La cooperación jurídica y judicial internacional

1. Los Estados partes deberían facilitar la cooperación entre sí de conformidad con la convención o el principio de reciprocidad para intercambiar información con el fin de prevenir la comisión de delitos informáticos, prestar ayuda en la investigación de dichos delitos y localizar a sus autores.

2. Los Estados partes deberían cooperar en la mayor medida posible, de conformidad con lo dispuesto en el presente artículo y en cumplimiento de otros instrumentos internacionales relativos a la cooperación internacional en materia penal, y en consonancia con el principio de reciprocidad, así como con la legislación nacional pertinente, con miras a prevenir, reprimir, detectar y enjuiciar los delitos relacionados con la utilización de las TIC.

3. A los efectos de la extradición y la asistencia judicial recíproca en materia penal, ninguno de los delitos contemplados en la convención debería considerarse delito político. Por lo tanto, una solicitud de extradición o de asistencia jurídica en materia penal en relación con ese delito no podrá ser rechazada por el hecho de tratarse de un delito político, un delito relacionado con un delito político o un delito cometido por motivos políticos.

5. Jurisdicción

Cada Estado debe adoptar las medidas necesarias para extender su jurisdicción a los delitos mencionados anteriormente, cuando:

a) el delito se cometa o se efectúe total o parcialmente en el territorio del Estado parte;

b) el delito se cometa o se efectúe total o parcialmente a bordo de un buque que enarbole el pabellón del Estado parte;

c) el delito se cometa o se efectúe total o parcialmente a bordo de una aeronave registrada conforme a las leyes del Estado parte;

d) el delito sea cometido o efectuado total o parcialmente por un nacional de un Estado parte si el delito es punible según la legislación nacional en el lugar de su comisión, o cuando se haya cometido en un lugar no sometido a la jurisdicción de ningún Estado;

e) el delito afecte a uno de los intereses superiores del Estado.

6. Extradición

a) Los delincuentes deberían ser entregados de un Estado a otro entre los Estados partes por los delitos antes mencionados, siempre que los delitos sean punibles según la legislación de los Estados partes de que se trate. Un Estado parte cuya legislación lo permita podrá aceptar una solicitud de extradición de una persona por un delito contemplado en la convención que no sea punible con arreglo a su legislación nacional.

b) Los delitos enunciados anteriormente deberían considerarse como delitos que dan lugar a extradición para los delincuentes que los cometen con arreglo a todo tratado de extradición existente entre los Estados partes.

c) Si un Estado parte que supedita la extradición a la existencia de un tratado recibe una solicitud de extradición de otro Estado parte con el que no lo vincula ningún tratado de extradición, podrá considerarse que la convención es una base jurídica para la extradición.

d) Una extradición debería estar sujeta a las condiciones estipuladas en la legislación del Estado parte requerido o a las condiciones definidas en los tratados de extradición aplicables, incluso en lo que respecta a los motivos por los que el Estado parte puede rechazar la solicitud.

e) Cada Estado parte podrá abstenerse de extraditar a sus ciudadanos, en cuyo caso debería, dentro de los límites de su jurisdicción, inculpar a aquellos de sus ciudadanos que cometan, en cualquier otro Estado parte, delitos punibles conforme a la legislación de ambos Estados partes con una pena de privación de libertad, si el otro Estado parte le remite una solicitud de enjuiciamiento de dicho ciudadano, acompañada de los expedientes, los documentos, la información y las pruebas que obren en su poder. El Estado parte requirente debería ser informado del curso dado a su solicitud, y se debería determinar la nacionalidad del delincuente en la fecha en que se cometió el delito por el que se solicita la extradición.

f) Los Estados partes deberían procurar, con sujeción a su legislación nacional, agilizar los procedimientos de extradición y simplificar los requisitos probatorios correspondientes con respecto a cualquiera de los delitos a los que se aplica el presente artículo.

g) A reserva de lo dispuesto en su legislación nacional y en sus tratados de extradición, un Estado parte requerido podrá, tras haberse cerciorado de que las circunstancias lo justifican y tienen carácter urgente, y a solicitud del Estado parte requirente, proceder a la detención de la persona presente en su territorio cuya extradición se pide, o adoptar otras medidas adecuadas para garantizar la comparecencia de esa persona en los procedimientos de extradición.

h) Si una solicitud de extradición presentada con el propósito de que se cumpla una condena es denegada por el hecho de que la persona cuya extradición se solicita es nacional del Estado parte requerido, éste debería —si lo permite su legislación nacional y de conformidad con ella— considerar, a petición del Estado parte requirente, la posibilidad de hacer cumplir la condena impuesta en virtud de la legislación nacional de la parte requirente, o el resto pendiente de dicha condena.

i) En todas las etapas de las actuaciones se debería garantizar un trato justo a toda persona contra la cual se lleve a cabo un procedimiento en relación con cualquiera de los delitos a los que se aplica el presente artículo, incluido el goce de todos los derechos y garantías previstos por la legislación nacional del Estado parte en cuyo territorio se encuentre esa persona.

j) Nada de lo dispuesto en la convención debería interpretarse como la imposición de una obligación de extraditar si el Estado parte requerido tiene motivos justificados para presumir que la solicitud de extradición se ha presentado con el fin de perseguir o castigar a una persona en razón de su sexo, raza, idioma, religión o nacionalidad, o que su cumplimiento podría perjudicar a la situación de esa persona por cualquiera de esas razones.

k) Los Estados partes no deberían poder rechazar una solicitud de extradición simplemente porque el delito esté relacionado con asuntos financieros.

l) Antes de denegar la extradición, el Estado parte requerido, de ser necesario, debería consultar al Estado parte requirente para darle amplia oportunidad de presentar sus opiniones y de proporcionar información pertinente en relación con los hechos expuestos en su solicitud.

m) Cada Estado parte debería, en el momento de depositar su instrumento de ratificación o adopción, tener la obligación de notificar a un organismo especializado, que se ha de acordar, la información de contacto de la autoridad responsable de las solicitudes

de extradición o de medidas procesales de arresto y de mantener periódicamente actualizada esa información ante dicho organismo.

7. Asistencia recíproca

a) Todos los Estados partes deberían prestarse asistencia recíproca en la mayor medida posible a los efectos de las investigaciones, los procedimientos relativos a los delitos relacionados con la información y la tecnología de la información o la reunión de pruebas electrónicas de los delitos.

b) La solicitud de asistencia bilateral y las comunicaciones conexas deberían presentarse por escrito. Cada Estado parte podrá, en casos de emergencia, presentar una solicitud urgente, incluso por correo electrónico, siempre y cuando dichas comunicaciones sean razonablemente seguras (incluyendo el uso de cifrado) y estén referenciadas, y se confirme la transmisión conforme a lo solicitado por el Estado parte.

c) Salvo en los casos previstos en la convención, la asistencia bilateral debería estar sujeta a las condiciones estipuladas en la legislación de la parte requerida o en los tratados de asistencia recíproca, incluidos los motivos por los cuales la parte requerida puede negarse a cooperar.

d) Cuando el Estado parte al que se solicita la asistencia recíproca solo puede prestarla si existe doble incriminación, la condición de doble incriminación debería considerarse cumplida independientemente de que la legislación del Estado parte clasifique el delito de que se trate en la misma categoría que el Estado parte requirente.

8. Suministro de información *motu proprio*

Un Estado parte podrá, de conformidad con su legislación nacional y sin que lo solicite previamente otro Estado parte, transmitir la información recopilada durante su propia investigación si considera que la divulgación de dicha información podría ayudar a ese otro Estado parte a iniciar o realizar una investigación relativa a los delitos tipificados como tales en la convención, o podría dar lugar a una solicitud de cooperación emitida por ese Estado parte.

9. Procedimientos relacionados con las solicitudes de cooperación y asistencia recíproca

a) Los apartados de este párrafo deberían aplicarse en ausencia de un tratado o convenio de asistencia recíproca y cooperación entre el Estado parte requirente y el Estado parte requerido sobre la base de la legislación vigente. En caso de que exista un tratado o convenio de ese tipo, dichos apartados no deberían aplicarse a menos que las partes interesadas acuerden aplicarlos en su totalidad o en parte.

b) Cada Estado parte debería designar a una autoridad central encargada de transmitir, recibir y aprobar solicitudes de asistencia judicial recíproca o de remitirlas a la autoridad competente. La información de contacto de la autoridad central debería actualizarse periódicamente.

c) Las solicitudes de asistencia recíproca a las que se refiere este artículo deberían atenderse de conformidad con los procedimientos especificados por el Estado parte requirente, siempre que no sean incompatibles con la legislación del Estado parte requerido.

d) El Estado parte requerido podrá aplazar la adopción de medidas en respuesta a la solicitud si dichas medidas pueden afectar a las investigaciones penales que estén llevando a cabo sus autoridades.

e) Antes de denegar o aplazar la asistencia, el Estado parte requerido debería determinar si accede a la solicitud en parte o con sujeción a las condiciones que juzgue apropiadas, previa consulta con el Estado parte requirente.

f) El Estado parte requerido debería informar al Estado parte requirente de los resultados de la ejecución de la solicitud. En caso de que la solicitud fuera denegada o su

ejecución definitiva aplazada, el Estado parte requerido debería tener la obligación de notificar al Estado parte requirente los motivos de dicha denegación o aplazamiento importante.

g) El Estado parte requirente podrá solicitar al Estado parte requerido que mantenga la confidencialidad de una solicitud solamente en la medida en que sea compatible con el cumplimiento de la misma. Si el Estado parte requerido no pudiera acceder al pedido de confidencialidad, lo debería hacer saber al Estado parte requirente. Acto seguido, este último debería decidir en qué medida se puede cumplir la solicitud.

h) En casos de emergencia, las solicitudes de asistencia recíproca podrán ser enviadas directamente a las autoridades judiciales del Estado parte requerido por sus homólogas del Estado parte requirente. En esos casos, la autoridad central del Estado parte requirente deberá enviar al mismo tiempo una copia de la solicitud a su homóloga del Estado parte requerido.

i) Las comunicaciones y solicitudes presentadas en virtud del párrafo anterior podrán realizarse por conducto de la Organización Internacional de Policía Criminal (INTERPOL).

10. Negativa a prestar asistencia

a) Un Estado parte requerido podrá negarse a prestar asistencia si considera que el cumplimiento de lo solicitado violaría su soberanía, su seguridad, su orden o sus intereses fundamentales, además de negarse a prestar asistencia por los motivos de denegación mencionados en los párrafos anteriores.

b) Una solicitud de asistencia judicial relativa a delitos mencionados en la convención no debería ser denegada por considerarse que los delitos son delitos políticos o de índole similar.

11. Confidencialidad y restricciones al uso

En ausencia de un tratado o convenio relativo a la asistencia recíproca entre el Estado parte requirente y el Estado parte requerido basado en la legislación vigente, deberá aplicarse el presente artículo. No debería aplicarse de existir tal convenio o tratado, a menos que los Estados partes interesados acuerden aplicarlo, en totalidad o en parte.

12. Aseguramiento expedito de la información almacenada mediante las TIC

a) Todo Estado parte podrá solicitar a otro Estado parte que salvaguarde con carácter urgente la información almacenada mediante una tecnología de la información ubicada en su territorio y respecto de la cual el Estado parte requirente desee presentar una solicitud de asistencia recíproca para buscar, incautar, asegurar o revelar la información.

b) Un Estado parte requerido podrá negarse a ejecutar una solicitud de aseguramiento si considera que ello amenazaría su soberanía, su seguridad, su orden o sus intereses.

13. Si el Estado parte requerido descubre —en el contexto de la ejecución de una solicitud de aseguramiento de parámetros técnicos del tráfico relativos a determinadas comunicaciones— que un proveedor de servicios de otro Estado ha participado en la transmisión de la información, debería revelar al Estado parte requirente una cantidad suficiente de parámetros técnicos del tráfico que permita identificar a ese proveedor de servicios y la vía por la que se transmitió la información cuyo aseguramiento se solicita.

14. Cooperación y asistencia bilaterales relacionadas con el acceso a información almacenada mediante las TIC

a) Todo Estado parte podrá solicitar a otro Estado parte que busque, consulte, incaute, asegure o divulgue información almacenada mediante las TIC y localizada en el territorio del Estado parte requerido, incluida la información que haya sido asegurada.

b) El Estado parte requerido debería tener la obligación de cumplir con el Estado parte requirente de conformidad con las disposiciones de la convención.

c) La respuesta a la solicitud debería tener carácter urgente si la información de que se trate puede ser objeto de pérdida o modificación.

15. Acceso transfronterizo a la información almacenada mediante las TIC

Todo Estado parte podrá, sin obtener la autorización de otro Estado parte, acceder a la información almacenada mediante las TIC que esté a disposición del público (código abierto), independientemente de la ubicación geográfica de la información.

16. Cooperación y asistencia bilaterales para la recopilación en tiempo real de parámetros técnicos del tráfico

a) Los Estados partes deberían prestarse asistencia bilateral en lo que respecta a la recopilación en tiempo real de parámetros técnicos del tráfico asociados a determinadas comunicaciones en sus territorios y transmitidos por medio de tecnologías de la información.

b) Cada Estado parte debería prestar esa asistencia, al menos en relación con los delitos respecto de los cuales la recopilación en tiempo real de esos parámetros sea factible para casos análogos en virtud de la legislación nacional.

17. Cooperación y asistencia bilaterales en materia de datos sobre el contenido

Los Estados partes deberían tener la obligación de prestarse asistencia bilateral en relación con la recopilación en tiempo real de datos sobre el contenido de determinadas comunicaciones transmitidas mediante tecnologías de la información, en la medida en que lo permitan los tratados y la legislación nacional aplicables.

18. Organismo especializado

a) Cada Estado parte debería garantizar, de conformidad con los principios básicos de su ordenamiento jurídico, la existencia de un organismo especializado, dedicado las 24 horas del día, los siete días de la semana, a prestar asistencia de forma inmediata a los fines de las investigaciones o los procedimientos relacionados con delitos vinculados a las tecnologías de la información o para la obtención de pruebas en forma electrónica con respecto a un determinado delito. Dicha asistencia debería incluir la facilitación o realización de lo siguiente:

i) la prestación de asesoramiento técnico;

ii) el aseguramiento de la información sobre la base de los artículos pertinentes;

iii) la reunión de pruebas, el suministro de información jurídica y la determinación del paradero de los sospechosos.

b) El organismo especializado de cualquier Estado parte debería tener la capacidad de comunicarse con carácter urgente con organismos similares de otros Estados partes.

c) Si el organismo especializado designado por un Estado parte no es una de las autoridades de ese Estado responsables de la asistencia bilateral internacional, el organismo especializado debería estar facultado para coordinar su labor de manera expedita con esas autoridades.

d) Cada Estado parte debería garantizar la disponibilidad de recursos humanos cualificados para facilitar la labor del mencionado organismo.

VI. Asistencia técnica y formación

1. Principios generales de la asistencia técnica

a) Los Estados partes deberían considerar la posibilidad de prestarse mutuamente la más amplia asistencia técnica, especialmente en beneficio de los países en desarrollo, en

relación con sus respectivos planes y programas de lucha contra los delitos relacionados con las TIC, incluidos el apoyo material y la capacitación en los ámbitos mencionados en la convención, así como la formación, la asistencia, la transferencia de tecnología y conocimientos y el intercambio de las mejores experiencias y conocimientos especializados pertinentes, lo que facilitará la cooperación internacional entre los Estados partes en materia de extradición y asistencia jurídica recíproca.

b) Los Estados partes deberían intensificar los esfuerzos para maximizar la eficacia de las actividades operacionales y de capacitación en las organizaciones internacionales y regionales y en el marco de los acuerdos o arreglos bilaterales y multilaterales pertinentes.

c) Los Estados partes deberían considerar la posibilidad de ayudarse entre sí, previa solicitud, a realizar evaluaciones, estudios e investigaciones sobre los tipos, las causas y las consecuencias de los delitos en el ámbito de las TIC en sus respectivos países, a fin de elaborar, con la participación de las autoridades competentes y los principales agentes, estrategias y planes de acción para combatir esos tipos de delitos.

d) Los Estados partes deberían considerar la posibilidad de establecer mecanismos de financiación con el fin de proporcionar asistencia a los esfuerzos realizados por los países en desarrollo mediante programas y proyectos de asistencia técnica.

e) Los Estados partes deberían considerar la posibilidad de intercambiar información sobre los avances jurídicos, normativos o tecnológicos relacionados con la ciberdelincuencia y la reunión de pruebas en formato electrónico.

2. Capacitación y creación de capacidad

a) Cada Estado parte debería, en la medida necesaria, elaborar, aplicar o perfeccionar programas de capacitación específicos para el personal encargado de prevenir y combatir los delitos relacionados con las TIC. Estos programas de capacitación podrían abarcar, entre otras, las siguientes esferas:

i) medidas eficaces para prevenir, detectar, investigar, sancionar y combatir los delitos en el ámbito de las tecnologías de la información y las comunicaciones, incluidos métodos electrónicos de reunión y utilización de pruebas y técnicas de investigación electrónicas;

ii) prevención de la transferencia del producto de los delitos tipificados con arreglo a la convención, así como recuperación de dicho producto;

iii) detección y suspensión de las transacciones vinculadas a la transferencia del producto de delitos tipificados con arreglo a la convención; vigilancia del movimiento del producto de los delitos tipificados como tales en la convención; vigilancia de los métodos utilizados para la transferencia, ocultación o disimulación de dicho producto;

iv) establecimiento de mecanismos y métodos legales y administrativos apropiados y eficientes para facilitar la incautación y el decomiso del producto de delitos tipificados con arreglo a la convención;

v) métodos utilizados para proteger a las víctimas y los testigos que cooperen con las autoridades judiciales y las fuerzas del orden;

vi) elaboración y planificación de una política estratégica para contrarrestar los delitos relacionados con las TIC. Los países deberían invertir en la creación y mejora de la capacidad forense digital, entre otras cosas proporcionando capacitación y cualificación en materia 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;

vii) preparación de solicitudes de asistencia judicial recíproca que satisfagan los requisitos de la convención;

viii) la investigación de delitos cibernéticos, la gestión de pruebas electrónicas, la cadena de custodia y el análisis forense;

ix) el suministro de formación lingüística y profesional en todas las actividades relativas a la lucha contra los delitos relacionados con las TIC y protección y agilización de la comunicación con los organismos especializados para detectar y combatir los delitos conexos;

b) Los Estados partes que dispongan de capacidades e infraestructuras más avanzadas en el ámbito de la ciberdelincuencia deberían asumir responsabilidades acordes con esas capacidades al prestar asistencia jurídica a otros Estados, especialmente a países en desarrollo, y al proporcionarles apoyo y asesoramiento y transferirles conocimientos en la esfera de la lucha contra la ciberdelincuencia.

Estados Unidos de América

[Original: inglés]
[28 de octubre de 2021]

El Gobierno de los Estados Unidos de América se complace en responder a la invitación formulada a los Estados Miembros para que presenten sus opiniones sobre el ámbito de aplicación, los objetivos y la estructura (los elementos) de la nueva convención, con respecto a la aplicación de las resoluciones 74/247 y 75/282 de la Asamblea General. Los Estados Unidos esperan con interés cooperar con otros Estados Miembros y partes interesadas para redactar un instrumento mundial orientado a mejorar la investigación y el enjuiciamiento de la ciberdelincuencia, en un marco de respeto de los derechos y obligaciones vigentes y basándose en ellos. Reiteran la importancia de mantener un proceso abierto, inclusivo, transparente y multipartito que permita a los Estados Miembros negociar de buena fe soluciones prácticas, basadas en el consenso y bien fundamentadas que, a nuestro juicio, alentarán la adhesión generalizada a un nuevo instrumento mundial de lucha contra la ciberdelincuencia.

El plazo propuesto para nuestro trabajo sería excesivamente breve, incluso en circunstancias normales, pero nuestra labor actual se realizará con el trasfondo de una pandemia mundial. Por ello, resulta aún más esencial realizar actividades focalizadas y eficientes para negociar un instrumento mundial contra la ciberdelincuencia. Por desgracia, en momentos en que gran parte del mundo se aboca a combatir la pandemia de COVID-19, los ciberdelincuentes explotan los consiguientes cambios que se han producido en el mundo y la dependencia de las tecnologías digitales. En todo el mundo la ciberdelincuencia es una amenaza directa para la seguridad y el bienestar de sociedades y personas. Se coopera desde hace tiempo para aumentar la capacidad colectiva de combatir esa explotación de las circunstancias, y podemos seguir reforzando esos logros mediante un examen minucioso de soluciones prácticas. Como la ciberdelincuencia representa una amenaza inmediata, resulta aún más imprescindible impulsar una labor centrada y resuelta para negociar un instrumento mundial de lucha contra ella.

Dicho instrumento de lucha contra la ciberdelincuencia debería orientarse a mejorar la cooperación internacional y crear recursos prácticos destinados a preparar a los organismos nacionales de aplicación de la ley para combatir la ciberdelincuencia, como se ha hecho mediante otros instrumentos de las Naciones Unidas respecto de otras formas de delincuencia transnacional, como la corrupción, el tráfico de estupefacientes, la trata de personas y el tráfico de migrantes. Además, debería garantizar que las autoridades nacionales puedan obtener y reunir pruebas electrónicas relativas a todo tipo de delitos, no solo los basados en la cibernética, así como promover la cooperación internacional en

dichos casos. Como todos los instrumentos de las Naciones Unidas contra la delincuencia, la convención debería establecer limitaciones y salvaguardias apropiadas, en el contexto de los marcos nacionales en vigor, relativas a la privacidad y las libertades civiles, en un marco de respeto pleno de los derechos humanos. Asimismo, el instrumento de lucha contra la ciberdelincuencia debería satisfacer la creciente necesidad de asistencia técnica y prever mecanismos para que los Estados Miembros la soliciten.

Al iniciar los Estados Miembros la labor de redacción es indispensable reconocer que no actuamos en el vacío. Tan importante como decidir el contenido del instrumento es reconocer lo que no corresponde incluir en él. En las Naciones Unidas y en otros foros intergubernamentales y multilaterales se está llevando a cabo una labor valiosa sobre otros asuntos relativos a la cibernética, que exceden el ámbito de la ciberdelincuencia. Es importante no duplicar ni menoscabar esa labor, para evitar conflictos de obligaciones y no perder de vista nuestro objetivo de elaborar un instrumento práctico y específico para combatir el delito cibernético. Si se intenta abordar en este instrumento de justicia penal todas las cuestiones relativas a la ciberdelincuencia, se corre el riesgo de sumir las negociaciones en debates vagos y tangenciales, que contribuirían poco a la lucha contra la ciberdelincuencia y se limitarían a retrasar nuestro avance hacia la elaboración de un instrumento útil.

En particular, en un instrumento sobre la delincuencia destinado a combatir el delito cibernético, los Estados Miembros no deberían incursionar en asuntos generales relativos a la cibergobernanza o la ciberseguridad. Aunque con frecuencia se consideran dos aspectos de un mismo asunto, la aplicación de las leyes en materia de ciberdelincuencia corresponde, en lo esencial, a los Gobiernos, en tanto que la ciberseguridad compete a una gran diversidad de agentes públicos y privados. El mandato del Comité Especial encargado de Elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos se centra en redactar un instrumento de justicia penal sobre asuntos penales para facilitar la adopción de medidas internacionales contra la ciberdelincuencia, en el que se definan los actos delictivos que se cometen en el ciberespacio y se prevean sanciones para ellos. El Comité Especial no tiene el mandato de fijar normas globales aplicables a las conductas no delictivas en línea. Incorporar los conceptos de cibergobernanza y ciberseguridad en un tratado sobre la ciberdelincuencia no cumpliría el objetivo de elaborar un instrumento sencillo y eficaz que recibiera apoyo amplio de los Estados Miembros.

Como se reafirmó en la resolución 75/282 de la Asamblea General, es indispensable que las negociaciones de un nuevo instrumento de lucha contra la ciberdelincuencia no entorpezcan los mecanismos existentes, como los instrumentos multinacionales y regionales que ya prevén diversos medios para combatir eficazmente ese problema. La mejor forma de lograr un consenso sobre este instrumento nuevo y evitar problemas políticos y divisiones es remitirnos a los que están en vigor y han resultado fructíferos. Deberíamos orientarnos por los logros alcanzados en la aplicación de otros tratados de justicia penal de las Naciones Unidas, como la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional. Esa convención ha sido de suma utilidad, porque se centra en tipos básicos de actividades delictivas organizadas, y contiene también disposiciones amplias sobre cooperación internacional que podrían aplicarse a la lucha contra cualquier tipo de delito grave cometido con fines de lucro por tres o más personas. Por ello, las partes han utilizado la Convención miles de veces con buenos resultados, incluso para combatir delitos como el uso de programas secuestradores y la explotación sexual de niños.

Los Estados Unidos reiteran, una vez más, la importancia de mantener un proceso abierto, inclusivo, transparente que permita a los Estados Miembros y otros interesados negociar de buena fe soluciones prácticas, basadas en el consenso y bien fundamentadas que, a nuestro juicio, alentarían a que se produjera una adhesión generalizada a un nuevo instrumento mundial de lucha contra la ciberdelincuencia.

Tipificación de los delitos cibernéticos básicos

En primer lugar, y lo que es más importante, todo instrumento nuevo debería establecer un mandato nacional para obtener y reunir pruebas electrónicas relativas a cualquier tipo de delito. Ello es imprescindible para que los países investiguen y enjuicien con eficacia casi todas las categorías de delitos, habida cuenta de que en la actualidad son muy pocos los que se cometen totalmente fuera del ámbito digital. Además, el instrumento debería facilitar la cooperación internacional para intercambiar pruebas electrónicas relativas a cualquier acto delictivo, sujeta a una disposición flexible sobre la doble incriminación como la que contienen la Convención contra la Delincuencia Organizada y la Convención de las Naciones Unidas contra la Corrupción[1].

Además, para que la cooperación internacional sea eficaz los Estados Miembros deben tener legislación apropiada por la que se tipifiquen los delitos cibernéticos básicos. A fin de evitar que los delincuentes dispongan de refugios seguros, es indispensable que entre los Estados Miembros haya una comprensión común de los delitos sustantivos básicos y de las facultades procesales de apoyo. Algunos estudios de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) indican que los países suelen estar de acuerdo en general acerca de las conductas básicas que deberían tipificarse como delito en las leyes específicas sobre ciberdelincuencia, y muchos acuerdos multinacionales y leyes penales nacionales contienen disposiciones comunes. Del mismo modo, hay una comprensión internacional ya establecida acerca de qué tipos de facultades procesales deben preverse para las autoridades a fin de respaldar la investigación eficaz de los delitos cibernéticos. Así pues, los profesionales tienen acumulados dos decenios de experiencia diversa sobre la investigación de la ciberdelincuencia que demuestra que las facultades sustantivas y procesales que se prevén comúnmente para investigar la ciberdelincuencia siguen siendo viables.

Un nuevo instrumento de lucha contra la ciberdelincuencia debería definir los delitos basados en la cibernética —delitos cuyo objetivo son las computadoras o los datos—, así como determinados delitos facilitados por la cibernética —aquellos en que se utiliza una computadora para facilitar su comisión— y aplicarse a ellos. La primera de esas dos categorías de delitos que se definiría en el nuevo instrumento, que es la principal, comprende los delitos que no pueden cometerse sin el uso no autorizado de computadoras o sistemas de redes y que por ello no existían como delito antes de la aparición de los sistemas informáticos. Los delitos basados en la cibernética pueden cometerse completamente en el ámbito digital. En el caso de los tipos básicos de delitos basados en la cibernética, como los ataques de denegación de servicio o el daño a computadoras y datos, se requieren leyes específicas, porque en la mayoría de las jurisdicciones la legislación penal se interpreta de manera estricta, y las leyes tradicionales que se refieren a conceptos conocidos, como la violación de domicilio y el vandalismo, suelen ser inadecuadas para aplicarse a la ciberdelincuencia. Además, algunas disposiciones del código penal que son aplicables a los delitos cometidos fuera de una red informática tal vez no puedan aplicarse con facilidad a los actos realizados mediante computadoras.

Más bien, deberíamos cuidar de no tratar los delitos tradicionales como "ciberdelincuencia" por el mero hecho de que para planificarlos o cometerlos se haya utilizado una computadora. Aunque se utilice ilícitamente una computadora para cometer un delito, algunas de las conductas delictivas pueden estar comprendidas en la legislación general, porque no tiene nada de particular ni singular que para incurrir en ellas se recurra a un sistema informático. En cambio, es correcto incluir algunos delitos facilitados por la

[1] Véanse el artículo 18, párr. 9, de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y el artículo 46, párr. 9, de la Convención de las Naciones Unidas contra la Corrupción. Aunque esas dos disposiciones difieren un poco entre sí, ambas dan al Estado parte requerido un margen de discrecionalidad considerable para prestar asistencia, en particular cuando se trata de la aplicación de medidas coercitivas.

cibernética en un instrumento contra la ciberdelincuencia, por ejemplo, en los casos en que utilizar una computadora aumente:

a) el alcance del delito, por ejemplo, si afecta a miles de víctimas o consiste en el robo de millones de registros de datos de pago;

b) la rapidez del ataque, porque una computadora aumenta exponencialmente la capacidad de cometer el delito;

c) la magnitud de los daños o perjuicios a las víctimas, o

d) el anonimato del autor.

Al aplicar esos conceptos, también podría ser razonable considerar que algunos delitos tradicionales, como el fraude y la explotación de niños, corresponden al ámbito de estas negociaciones. Sin embargo, los Estados Miembros deberían ser cautelosos respecto de la amplitud de las categorías de delitos cibernéticos que se proponen abordar, para no distorsionar conceptos de justicia penal ya establecidos. Las leyes y los instrumentos establecidos desde hace tiempo no pierden su aplicabilidad por el mero hecho de que determinado delito tenga algún componente “cibernético”.

Además, un instrumento mundial de lucha contra la ciberdelincuencia debería requerir que las partes promulgaran leyes que tipificaran los delitos cibernéticos básicos utilizando terminología tecnológicamente neutra, y garantizando al mismo tiempo las salvaguardias procesales. Tipificar los delitos de manera tecnológicamente neutra (es decir, penalizar las actividades que afectan a la confidencialidad, la integridad y la disponibilidad de los datos informáticos en lugar de la forma o el método concreto utilizado, como el *phishing* o los programas secuestradores) garantizaría que las disposiciones penales sustantivas abarcaran no solo las tecnologías y técnicas delictivas actuales, sino también las futuras. A modo de ejemplo de la rapidez con que evoluciona la tecnología, incluso el proyecto de estudio exhaustivo sobre la ciberdelincuencia de 2013, que procuraba expresamente ser exhaustivo, no contenía información detallada sobre tecnologías o técnicas que no se utilizaban ampliamente o que acababan de aparecer a la fecha de la redacción del proyecto de estudio, como los programas secuestradores, la Internet de las cosas y las criptomonedas, ni se refería a la velocidad con que se desarrollaba y se estaba imponiendo la tecnología móvil. Reconociendo ese problema, una de las conclusiones y recomendaciones acordadas por los Estados Miembros en la reunión del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético fue que los Estados Miembros debían velar por que sus disposiciones legislativas resistieran el paso del tiempo frente a futuros avances tecnológicos promulgando leyes cuya formulación fuera neutral tecnológicamente y que penalizaran las actividades consideradas ilícitas en lugar de los medios utilizados[2]. Ello es especialmente importante en momentos en que procuramos redactar un instrumento duradero que abarque suficientemente las tecnologías futuras y satisfaga las necesidades de los profesionales encargados de la aplicación de la ley tanto en la actualidad como en el futuro.

Teniendo en cuenta estos principios, un instrumento mundial contra la ciberdelincuencia debería tipificar como delito, entre otros, los siguientes actos:

a) el acceso ilícito, es decir, el acto de acceder a una computadora o a un sistema informático sin autorización;

b) la interceptación ilícita, es decir, la interceptación ilegal y en tiempo real del contenido de las comunicaciones o de los datos de tráfico relacionados con las comunicaciones;

[2] Véase el 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 (UNODC/CCPCJ/EG.4/2021/2).

c) la interferencia en datos o sistemas, es decir, el uso de programas maliciosos, los ataques de denegación de servicio, el uso de programas secuestradores y la eliminación o modificación de datos;

d) el abuso en la utilización de dispositivos, es decir, el tráfico o la utilización de datos de tarjetas de crédito, contraseñas e información personal que den acceso a los recursos;

e) los delitos en que se utilicen imágenes de abusos sexuales de niños;

f) los delitos relacionados con el fraude facilitado por la cibernética, es decir, la manipulación de sistemas o datos informáticos con fines fraudulentos, como la suplantación de identidad, el poner en riesgo los correos electrónicos de empresas y el fraude con las subastas;

g) los delitos relacionados con la violación de los derechos de propiedad intelectual y otros derechos conexos;

h) la tentativa de cometer un delito, la ayuda para cometerlo, la incitación a ello y la confabulación para cometerlo.

Además, se debería penalizar el blanqueo del producto de la ciberdelincuencia. Por último, las personas jurídicas deberían estar sujetas a sanciones penales o civiles y administrativas si participan en la comisión de los delitos cibernéticos previstos en el instrumento.

Facultades procesales para la reunión y el intercambio de pruebas electrónicas

Además de penalizar los delitos sustantivos, un instrumento mundial contra la ciberdelincuencia debería satisfacer la necesidad de que las autoridades nacionales reúnan, conserven e intercambien pruebas electrónicas, en un marco de respeto de las garantías procesales, los derechos humanos y las libertades fundamentales. Algunos Estados Miembros han señalado que las facultades procesales tradicionales previstas en su derecho interno tal vez no puedan ejercerse en el caso de datos intangibles o no permitan la reunión suficientemente rápida de pruebas electrónicas que son volátiles. Como siempre, si son anticuadas las leyes no bastarían para hacer frente a las numerosas dificultades que plantea la investigación de delitos electrónicos, en particular las relativas a tecnologías nuevas de uso extendido, como los servicios de cifrado y de computación en la nube. Por ello, para reunir pruebas electrónicas es indispensable contar con legislación que establezca facultades procesales especializadas. Esas leyes deberían redactarse teniendo en cuenta los conceptos técnicos pertinentes y las necesidades prácticas de quienes llevan a cabo la investigación penal. Concretamente, la legislación por la que se establezcan dichas facultades procesales debería prever lo siguiente:

a) la conservación rápida de los datos informáticos almacenados;

b) mandamientos de presentación de datos informáticos;

c) el registro a efectos de incautación de datos informáticos almacenados;

d) la reunión de datos de tráfico de comunicaciones en tiempo real; y

e) la reunión de datos de contenido en tiempo real, en casos de delitos graves.

Además, el nuevo instrumento debería favorecer la cooperación para obtener y reunir pruebas electrónicas relativas no solo a delitos cibernéticos, sino a cualquier tipo de delitos. Casi todos los delitos importantes suponen pruebas electrónicas, ya sea en forma de datos de telefonía móvil, correos electrónicos, datos relativos a operaciones y datos de otra índole, que sean de interés para su investigación y enjuiciamiento. Como cuestión interna, los Estados Miembros requieren marcos jurídicos modernos relativos a las pruebas que hagan admisibles las pruebas electrónicas en investigaciones y enjuiciamientos penales, y

permitan en particular el intercambio de estas con asociados de organismos extranjeros de aplicación de la ley.

Cooperación internacional

Además de en la legislación interna, toda cooperación internacional eficaz en materia de ciberdelincuencia se basa tanto en los conductos oficiales previstos para la cooperación en los tratados, por ejemplo los de asistencia judicial recíproca, como en otros canales, por ejemplo, la cooperación interpolicial tradicional que estuviera autorizada. La nueva convención contra la ciberdelincuencia debería aprovechar los mecanismos eficaces para aumentar la cooperación internacional establecidos conforme a los tratados en vigor, sin menoscabar dichos instrumentos ni las formas actuales de cooperación internacional en la lucha mundial contra el delito cibernético. Las disposiciones sobre cooperación internacional que figuren en la convención de lucha contra la ciberdelincuencia, en particular las relativas a la asistencia judicial recíproca, la extradición, el traspaso de la persecución penal de un órgano a otro, el decomiso del producto del delito —incluidas las monedas virtuales—, y su restitución a las víctimas, la doble incriminación y la cooperación en materia de aplicación de la ley, deberían adherirse estrictamente a las disposiciones de la Convención contra la Delincuencia Organizada y la Convención contra la Corrupción, como las relativas a las salvaguardias y los mecanismos de protección adecuados que figuran en ellas, que la gran mayoría de los Estados Miembros ha aplicado satisfactoriamente. Además, la disposición que se refiera a la asistencia judicial recíproca debería prever una asistencia de gran alcance para la obtención de pruebas electrónicas de un delito, se haya cometido o no utilizando un sistema informático.

Asistencia técnica y creación de capacidad

Algunos estudios de la UNODC indican que más del 75 % de los países tiene en sus organismos de aplicación de la ley dependencias especiales que se ocupan de asuntos relacionados con la ciberdelincuencia, y alrededor del 15 % un organismo especializado y dedicado a los delitos cibernéticos. Ello pone de relieve el carácter igualmente especializado de la investigación de esos delitos, y en particular la necesidad de formación que también lo sea. Además, han aumentado considerablemente la complejidad de los delitos cibernéticos y la de los elementos electrónicos o digitales de los delitos tradicionales, lo que aumenta la demanda de formación y retención de investigadores y expertos técnicos altamente cualificados.

La insuficiencia de la capacidad nacional es la razón más común por la que los países no pueden cooperar eficazmente a nivel internacional. En la mayoría de los países la cooperación internacional no se malogra por falta de voluntad, sino por las limitaciones de la legislación interna o la falta de conocimientos técnicos de los organismos de aplicación de la ley. Muchos Estados Miembros no tienen recursos suficientes para que esos organismos puedan ocuparse de la ciberdelincuencia o la gestión de pruebas electrónicas. Por ejemplo, debido a las prioridades nacionales que han fijado, algunos Estados Miembros tienen dificultades para capacitar a investigadores y peritos forenses y retenerlos, así como para reducir la escasez de equipo y programas informáticos. Por ello, hay amplio consenso internacional respecto de que la asistencia técnica y la creación de capacidad para los organismos de aplicación de la ley, en particular sus investigadores, fiscales y jueces, siguen siendo los requisitos más urgentes para lograr una respuesta internacional eficaz a la ciberdelincuencia. Además, a medida que las pruebas electrónicas se convierten en un aspecto indispensable de la investigación de casi todos los tipos de delitos, incluso los funcionarios no especializados de esos organismos requerirán conocimientos básicos sobre investigaciones relacionadas con informática.

Las disposiciones de un instrumento sobre ciberdelincuencia relativas a la asistencia y la capacidad técnicas deberían prever:

a) medidas de los Estados Miembros para formular, desarrollar o perfeccionar programas de capacitación destinados al personal de sus servicios encargados de prevenir y reprimir la ciberdelincuencia;

b) que los Estados Miembros consideren, según sus capacidades y en el marco de sus respectivos planes y programas de lucha contra la ciberdelincuencia, la posibilidad de prestarse la más amplia asistencia técnica, especialmente en favor de los países en desarrollo y los países que puedan estar desproporcionadamente expuestos al delito cibernético;

c) la creación de mecanismos para apoyar la aplicación de un instrumento contra la ciberdelincuencia mediante contribuciones financieras voluntarias de los Estados Miembros;

d) que los Estados Miembros consideren la posibilidad de aportar contribuciones voluntarias al Programa Mundial contra el Delito Cibernético de la UNODC y las iniciativas conexas de la Oficina orientadas a crear capacidad en materia de justicia penal.

Participación de la sociedad, las entidades y las organizaciones

La lucha contra la ciberdelincuencia no puede ser una labor aislada, en razón de la complejidad y la naturaleza multifacética de ese problema. Un instrumento para combatir la ciberdelincuencia debería tener en cuenta —prestando la debida atención a la igualdad de género— que es importante que en la labor de prevención del delito cibernético participen activamente personas y grupos, como las organizaciones no gubernamentales, las organizaciones de la sociedad civil, las instituciones académicas y el sector privado. A través de esa participación se podría sensibilizar al público sobre las amenazas de la ciberdelincuencia, garantizar que la labor de los Estados Miembros se realice con transparencia y abordar las cuestiones sustantivas relacionadas con la privacidad, las libertades civiles y los derechos humanos. Además, la eficacia del instrumento dependerá de la contribución de personas y entidades con experiencia en el ámbito de la ciberdelincuencia. Para elaborar un instrumento de lucha contra la ciberdelincuencia que sea práctico y útil es imprescindible la participación activa de expertos en la materia.

Mecanismos de aplicación

Sería prematuro en este momento determinar si se requiere un proceso aparte para examinar la aplicación futura del instrumento y, en caso afirmativo, la forma que debería adoptar. Hay varios modelos de instrumentos eficaces que podrían tenerse en cuenta. Dado que los recursos para asistencia técnica son escasos, se debería considerar la posibilidad de utilizar mecanismos basados en opciones de bajo costo, con objeto de obtener el máximo de contribuciones posible de los donantes para la asistencia técnica. Uno de esos mecanismos consistiría en autorizar a la Comisión de Prevención del Delito y Justicia Penal, creada en virtud de la resolución 1992/1 del Consejo Económico y Social, para examinar todas las cuestiones relacionadas con los objetivos del instrumento de lucha contra la ciberdelincuencia. Un buen precedente de ese tipo de supervisión es el que se ha sentado en relación con la Comisión de Estupefacientes, que se ocupa de vigilar la aplicación de los tres tratados de fiscalización internacional de drogas. Como se señala en la sección anterior sobre la participación de la sociedad, las entidades y las organizaciones, es fundamental tener en cuenta la participación activa de la sociedad y de las entidades y organizaciones públicas cuando se trate de impulsar cualquier labor relacionada con el instrumento. Sin embargo, el debate sobre los mecanismos de aplicación debería aplazarse hasta que se defina mejor el ámbito de aplicación de la convención.

Federación de Rusia

Nota de la Secretaría: la presentación de la Federación de Rusia figura en el documento A/75/980, titulado “Carta de fecha 30 de julio de 2021 dirigida al Secretario General por el Encargado de Negocios interino de la Misión Permanente de la Federación de Rusia ante las Naciones Unidas”, y en el anexo de esa carta, titulado “Proyecto de Convención de las Naciones Unidas contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos”, que se puso a disposición de la Asamblea General en su septuagésimo quinto período de sesiones. Se transmite al Comité Especial encargado de Elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos en el marco de la presentación de las opiniones de los Estados Miembros sobre el ámbito de aplicación, los objetivos y la estructura (los elementos) de la nueva convención, conforme a la invitación de la Presidenta del Comité Especial.

Indonesia

[Original: inglés]
[28 de octubre de 2021]

Antecedentes y objetivos

Al ser uno de los mayores usuarios de Internet del mundo, Indonesia reconoce la importancia de las tecnologías de la información y las comunicaciones (TIC) para la sociedad. Sin embargo, los avances de esas tecnologías se han aprovechado en conductas irresponsables, sobre todo la ciberdelincuencia y el ciberterrorismo, lo que ha socavado la utilización de las TIC al servicio del desarrollo político, económico y social.

La ciberdelincuencia, al igual que otros delitos transnacionales, ha afectado a la comunidad internacional debido a la naturaleza singular y sin fronteras de la tecnología y el ciberespacio. Por consiguiente, la cooperación internacional es decisiva. Indonesia celebra la aprobación de la resolución 74/247 de la Asamblea General, en la que esta decidió establecer un comité intergubernamental especial de composición abierta a fin de elaborar una convención internacional integral sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos.

Indonesia considera muy oportuno y esencial debatir la convención específica sobre la ciberdelincuencia en el marco del Comité Especial encargado de Elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos, y confía en que los Estados aprovecharán el impulso para debatir y negociar un instrumento internacional capaz de responder a los retos de la ciberdelincuencia, de manera inclusiva y transparente.

A lo largo de la última década se han realizado importantes avances en el examen y la elaboración de instrumentos internacionales destinados a determinar los métodos más eficaces de prevención de la ciberdelincuencia. En consecuencia, al considerar un futuro instrumento relativo a la ciberdelincuencia, los Estados deberían tener en cuenta todas las plataformas y los marcos existentes, incluida la labor del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético y la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional.

El debate sobre la convención relativa a la ciberdelincuencia debería tener por principal finalidad mejorar y promover la cooperación internacional en apoyo de las iniciativas nacionales, regionales e internacionales de lucha contra la utilización de las TIC con fines delictivos, entre otras cosas proporcionando asistencia técnica para perfeccionar la legislación y los marcos nacionales de los Estados Miembros y reforzar la capacidad de sus autoridades nacionales para hacer frente a esos delitos.

Además, la convención debería prever medidas apropiadas y eficaces entre los Estados, así como, en su caso, para la colaboración con las organizaciones internacionales y regionales competentes.

Principios

Al igual que con muchos convenios internacionales, nuestras consideraciones deberían reflejar las obligaciones de los Estados Miembros de conformidad con los principios de igualdad soberana e integridad territorial de los Estados, así como de la no injerencia en los asuntos internos de otros Estados. Además, los Estados deberían respetar los derechos soberanos de otros Estados al elaborar políticas y leyes para luchar contra la ciberdelincuencia con arreglo a sus condiciones y necesidades nacionales.

En el futuro instrumento se deben reconocer las repercusiones en la seguridad y las consecuencias socioeconómicas y humanitarias de la utilización de las TIC con fines delictivos. Al mismo tiempo, la convención debe garantizar que las medidas de lucha contra la ciberdelincuencia se centren en las conductas delictivas y no pongan en peligro el desarrollo de las TIC, en particular en la investigación, el desarrollo y la transferencia de tecnología.

Promover la utilización de esas tecnologías con fines pacíficos redunda en interés de todos y es vital para el bien común. El respeto de la soberanía, los derechos humanos y las libertades fundamentales, así como el desarrollo sostenible y digital, siguen siendo aspectos fundamentales de esos esfuerzos.

Indonesia también estima conveniente velar por que los procedimientos penales se establezcan, implementen y apliquen de conformidad con el derecho interno de cada nación, al tiempo que reconoce la necesidad de abordar los desafíos planteados por las diferencias en los procedimientos penales de los Estados, así como las obligaciones de cada Estado dimanantes de los instrumentos internacionales pertinentes, como la Convención contra la Delincuencia Organizada y los tratados sobre derechos humanos internacionales, derechos de propiedad intelectual y extradición bilateral y asistencia jurídica recíproca.

Además, los Estados Miembros deben resaltar la necesidad de mantener un proceso abierto y transparente en el que participen múltiples interesados y que permita a todos los Estados Miembros negociar de buena fe en busca de soluciones fundamentadas, consensuadas y realistas.

Ámbito de aplicación

El ámbito de aplicación de la convención debe poder responder a los retos actuales y futuros que plantee la utilización indebida de las TIC con fines delictivos, proteger a los usuarios de esas tecnologías y mitigar y prevenir los daños a las personas, los datos, los sistemas, los servicios y las infraestructuras.

La convención también debe garantizar que los Estados Miembros puedan adoptar las medidas legislativas y de otra índole necesarias para tipificar como delito la realización de actividades prohibidas por la convención, en particular los delitos informáticos y los delitos relacionados con computadoras, y destinadas a otros fines ilícitos.

Indonesia considera que la futura convención debería abarcar una amplia serie de delitos cibernéticos fundamentales que incluyen, entre otros, los siguientes:

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

b) la interceptación ilícita de datos y sistemas informáticos;

c) el fraude;

d) la utilización indebida de datos y sistemas informáticos con fines delictivos;

e) la violación de los derechos de autor y derechos conexos;

f) la manipulación de datos y sistemas informáticos;

g) la distribución y transmisión de contenidos y materiales ilegales, por ejemplo, pornografía, pornografía infantil, desinformación, confabulación, bulos y material que encierre hostilidad por motivos de raza, nacionalidad, religión o políticos.

Los Estados Miembros deberían considerar la posibilidad de adoptar las medidas necesarias para llevar a cabo los procedimientos penales previstos en la convención, entre otras cosas:

a) el aseguramiento de datos y sistemas y la preservación de los parámetros técnicos de tráfico almacenados por uno o varios proveedores de servicios, teniendo en cuenta que el plazo de conservación de los datos y la clasificación de los datos almacenados en su territorio están regulados por la legislación nacional y el derecho interno;

b) la presentación o transferencia de datos informáticos almacenados por personas físicas o jurídicas, y el establecimiento de medidas adecuadas para obligar a los proveedores de servicios de sistemas en línea a presentar o transferir datos informáticos almacenados, incluidos los datos relacionados con el tipo de servicios prestados;

c) la búsqueda e incautación de datos y sistemas informáticos, la creación y el aseguramiento de copias de datos informáticos, y la modificación y transferencia de datos almacenados;

d) la reunión y el registro de parámetros técnicos del tráfico en tiempo real, así como la obtención de esos parámetros de proveedores de servicios o sistemas en línea.

Teniendo en cuenta lo que antecede, los Estados Miembros deberían velar por que el proceso de investigación de la ciberdelincuencia se lleve a cabo de conformidad con los principios de protección de la privacidad, confidencialidad, sostenibilidad del servicio público, mantenimiento de la continuidad de los servicios públicos y defensa del interés público, así como la integración de los datos.

Cooperación

La ciberdelincuencia y los delitos facilitados por la utilización de las TIC deberían investigarse eficazmente en los planos nacional y transnacional. Así pues, el instrumento debería cumplir la función de mecanismo eficaz de cooperación internacional en la lucha contra la utilización de las TIC con fines delictivos. Dicha colaboración debería llevarse a cabo sobre la base del beneficio mutuo y la reciprocidad de conformidad con la legislación nacional, teniendo en cuenta los instrumentos existentes y los mecanismos y marcos en vigor.

Dada la importancia de los enfoques basados en la participación de múltiples interesados para la prevención, detección y erradicación de la ciberdelincuencia, el debate debería centrarse también en el fomento de una sólida cooperación con las entidades que se ocupan de la ciberdelincuencia, incluida la cooperación entre las autoridades encargadas de hacer cumplir la ley y los proveedores de servicios de TIC. En este contexto, la colaboración con la empresa privada, reforzada por alianzas público-privadas cuando sea factible, es crucial para mejorar el conocimiento y aumentar la eficacia de las respuestas a la ciberdelincuencia. Los Estados Miembros también deberían invertir en la concienciación sobre la ciberdelincuencia en los sectores público y privado.

Nuestras deliberaciones también deberían poner de relieve medidas que permitan a las autoridades realizar investigaciones en las que se reúnan y confisquen datos mediante mecanismos de asistencia jurídica recíproca, y los Estados Miembros podrían considerar la posibilidad de utilizar sus marcos jurídicos existentes a este respecto.

Por lo que se refiere a la asistencia jurídica recíproca, en nuestras deliberaciones deberíamos tener en cuenta en la mayor medida posible las leyes, los tratados y los acuerdos pertinentes, con respecto a las investigaciones, los enjuiciamientos y las actuaciones judiciales. Se alienta a los Estados Miembros a que, entre otras cosas, estudien acuerdos para agilizar la recogida de pruebas electrónicas o mecanismos de intercambio de información entre las autoridades competentes.

Las disposiciones de la convención relativas a la cooperación internacional deben proporcionar un marco jurídico esencial para abordar los problemas de procedimiento, las lagunas e insuficiencias de los mecanismos de cooperación internacional, especialmente en relación con las investigaciones, el intercambio de información, la reunión de datos y pruebas electrónicas, y el enjuiciamiento, así como para facilitar la extradición entre Estados. También se anima a los Estados Miembros a designar puntos de contacto o autoridades para agilizar la aplicación de las disposiciones de la convención relativas a la cooperación internacional.

Además, los Estados Miembros podrían considerar la posibilidad de fortalecer su capacidad nacional para detectar e investigar la utilización de las TIC con fines delictivos y darle respuesta, mediante iniciativas de creación de capacidad y asistencia técnica que contribuyan a aumentar la resiliencia de los Estados Miembros. Estas medidas de creación de capacidad deberían basarse en la confianza mutua, estar impulsadas por la demanda que corresponde a necesidades detectadas a nivel nacional y reconocer plenamente la implicación nacional.

Dado que la colaboración en la prevención y erradicación de la ciberdelincuencia sigue siendo una prioridad en nuestros debates, el futuro instrumento debería incluir, como mínimo, una lista de actividades encaminadas a mejorar la cooperación mediante las siguientes medidas:

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 desarrollo de las competencias y los recursos humanos en relación con las políticas que permiten a los Estados Miembros aumentar la adaptabilidad a las tecnologías digitales;

g) 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;

Mediante este mecanismo, los Estados Miembros también deberían seguir aumentando la eficacia de la coordinación y las sinergias interinstitucionales nacionales, incluidos el intercambio de información y la interacción con las organizaciones regionales, el sector privado, los equipos informáticos de respuesta de emergencia y los equipos de respuesta a incidentes de ciberseguridad, las organizaciones de la sociedad civil y otros interesados para contribuir a la eficacia de la cooperación internacional.

El debate debería abarcar también un mecanismo de examen de la aplicación o ejecución de todos los compromisos y obligaciones que entrañe el futuro instrumento.

Jamaica

[Original: inglés]
[29 de octubre de 2021]

En cumplimiento de la solicitud de la secretaría del Comité Especial encargado de Elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos de que los Estados formularan observaciones sobre el ámbito de aplicación, los objetivos y la estructura de una convención internacional sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, se presentan las opiniones que figuran a continuación.

Jamaica espera con interés cooperar con otros Estados Miembros en la labor en curso para redactar una convención sobre la ciberdelincuencia. Prevé que se elabore un instrumento que sirva a la comunidad mundial procurando proteger a los ciudadanos de las ciberamenazas u otros ataques delictivos y que sea objeto de aceptación y ratificación universales. Valora la participación de expertos de la sociedad civil en esa esfera para orientar nuestras deliberaciones.

Jamaica considera que el proceso de redactar una convención sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones (TIC) con fines delictivos es un avance importante en la respuesta mundial a los problemas que supone dicha amenaza para los Estados. El objetivo de la convención se formuló con precisión en el informe que aprobó por consenso en 2015 el Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional, en cuyo párrafo 13 d) se señala que los Estados deberían estudiar cuál es la mejor manera de cooperar para intercambiar información, prestarse asistencia mutua, entablar acciones penales por el uso de las TIC con fines delictivos y aplicar otras medidas de cooperación para hacer frente a tales amenazas[3].

Cooperar mediante el intercambio de información para ayudar a los Estados a combatir y enjuiciar la utilización de las TIC con fines delictivos debería ser el objetivo general de la convención. De ello se desprende, a la vez, el objetivo de profundizar entre los Estados la comprensión de las distintas perspectivas que existen sobre la ciberdelincuencia. Se espera que ello conduzca a una armonización de los enfoques, creando un marco internacional que resulte útil para todos. Sin embargo, cumplir ese objetivo depende de un proceso en que se examinen las posturas de todos los Estados, entre ellos los pequeños Estados insulares en desarrollo, de manera equilibrada, imparcial, transparente e inclusiva.

Deberían tenerse en cuenta otros procesos que pueden contribuir, sin retrasarlo indebidamente, al avance hacia la elaboración de una convención. Para demostrar la importancia que atribuimos a la lucha contra la ciberdelincuencia, deberían cumplirse los plazos acordados para las negociaciones y la finalización del proyecto de convención.

Se entiende que el punto de partida de las negociaciones es la definición de los términos utilizados. Estos fijan el alcance de la convención y son importantes para cumplir los objetivos comunes de los participantes. Como tales, las definiciones deberían ser claras, precisas y minuciosas, para que no resulten demasiado restrictivas o amplias y se ajusten al contexto y las finalidades de la convención.

Combatir la utilización de las TIC con fines delictivos es un mandato amplio. Por ello, las definiciones de los delitos deberían concebirse de manera que puedan adaptarse a los

[3] A/70/174.

cambios futuros. Deberían formularse de modo que no se limiten a las tecnologías existentes, sino que sea posible interpretarlas con amplitud suficiente para adaptarlas a las tecnologías del futuro y al entorno de las TIC, que cambia constantemente.

En la convención deberían preverse delitos cuya represión fortalezca los instrumentos de que disponen los países para combatir la ciberdelincuencia y no vulnere los derechos y libertades fundamentales de las personas, sino procure promover el respeto de esos derechos. Por ello, se deberían tener en consideración los tratados internacionales de derechos humanos.

Las disposiciones de una nueva convención deberían tener debidamente en cuenta el principio de la soberanía de los Estados, así como otros principios enunciados en la Carta de las Naciones Unidas y en el derecho internacional, en materia de procedimiento penal, aplicación de la ley y cooperación internacional.

A juicio de Jamaica, en la convención se debería prestar atención suficiente a la cooperación internacional, porque ello fomentaría una mayor colaboración en la lucha mundial contra la ciberdelincuencia. Cuando no existiera un tratado de asistencia judicial recíproca entre Estados, la convención debería servirles de orientación sobre el procedimiento que debería seguirse para formular solicitudes y responder a ellas. Ello debería abarcar asuntos como la responsabilidad por los gastos.

La convención debería reconocer las diversas capacidades de los Estados, que a la vez repercuten en sus posibilidades de cooperar en la medida necesaria para obtener resultados óptimos. Por ello, es decisivo que se preste asistencia técnica para reforzar la capacidad de los Estados de contribuir más al marco mundial de la lucha contra la ciberdelincuencia. A ese respecto, la labor de fomento de la capacidad debería ser sostenible, tener propósitos claros, ajustarse a las necesidades nacionales y cumplir el objetivo de desarrollar los recursos humanos en ese ámbito especializado. También debería considerarse la posibilidad de establecer un mecanismo de financiación, a fin de apoyar las iniciativas de creación de capacidad para aplicar la convención sobre la ciberdelincuencia.

Japón

[Original: inglés]
[29 de octubre de 2021]

El Japón, en su calidad de Estado Miembro que considera importante llevar a cabo un proceso inclusivo, transparente e imparcial para redactar la convención de las Naciones Unidas sobre la ciberdelincuencia que se ha previsto elaborar, se complace en aportar su contribución a esa nueva convención antes de que comience su redacción oficial, y agradece la iniciativa de la Presidenta de ofrecer la posibilidad de hacerlo.

Aunque los distintos Estados enfrentan problemas diferentes en materia de ciberdelincuencia, el Japón considera que la ciberdelincuencia para todos los Estados Miembros una amenaza grave que cambia constantemente. Para combatir la ciberdelincuencia, que trasciende con facilidad las fronteras nacionales, es fundamental que todos los Estados Miembros cooperen entre sí. Por ello, el Japón considera que deberíamos aspirar a crear un ciberespacio libre, equitativo y seguro y aumentar nuestra capacidad de prevenir y combatir la ciberdelincuencia en todo el mundo, dando al contenido de la nueva convención internacional un carácter universal y aceptable para todos los Estados Miembros.

En las presentes observaciones se exponen los puntos de vista del Japón sobre el ámbito de aplicación, los objetivos y la estructura de la nueva convención, con el fin de promover el debate en el Comité Especial encargado de Elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos, establecido conforme a la resolución 74/247 de la Asamblea General.

Ámbito de aplicación

Para reforzar las medidas mundiales de lucha contra la ciberdelincuencia y establecer un marco internacional universal, la comunidad internacional debería, en primer lugar, elaborar un marco sólido, centrado en disposiciones básicas y esenciales relativas a los delitos y el procedimiento penal, así como en la asistencia judicial recíproca y otros tipos de cooperación internacional en este ámbito.

Los actos que se tipifiquen como delito en la nueva convención deberían limitarse a la ciberdelincuencia; los delitos previstos en ese instrumento deberían abarcar sobre todo los basados en la cibernética, pero los facilitados por la ciberdelincuencia deberían incluirse solo cuando se requiriera y si hubiera consenso general a ese respecto entre los Estados Miembros.

La nueva convención debería basarse resueltamente en los debates anteriores y en los que se llevan a cabo en los marcos existentes de la lucha contra la ciberdelincuencia, teniendo presentes al mismo tiempo las deliberaciones y la labor en otros foros en que se examina la ciberdelincuencia, para no duplicar ni entorpecer las actividades.

A fin de establecer un marco internacional universal que sea aplicable en general a todo uso que se haga de las tecnologías de la información y las comunicaciones, independientemente de las diferencias entre los Estados, y a fin de adaptarse a los cambios que se produzcan en el futuro en relación con esas tecnologías, las disposiciones de la nueva convención deberían formularse de manera tecnológicamente neutra.

Pese a la importancia que tiene combatir la ciberdelincuencia, las medidas de lucha contra ella no deberían ir en detrimento del principio del debido proceso ni limitar injustificadamente el ejercicio de los derechos humanos. Estas salvaguardias son condiciones previas para una cooperación internacional fructífera, y por ello la nueva convención debería contener disposiciones concretas que garantizaran el debido proceso y el respeto de los derechos humanos.

Objetivo

El objetivo principal de la nueva convención debería ser contribuir a la seguridad de todos quienes se ocupan de las tecnologías de la información y las comunicaciones que requieren protección, así como salvaguardar sus intereses. Ello puede lograrse reforzando las medidas contra la ciberdelincuencia a nivel mundial, mediante la creación de un marco internacional universal que se aplique del modo más amplio posible a ese fenómeno en sus diversas formas transnacionales, así como apoyando una cooperación bilateral o multilateral eficaz en las investigaciones y los procesos penales.

Para lograr ese objetivo, la nueva convención debería contener disposiciones básicas y esenciales que pueda cumplir y aplicar el mayor número posible de Estados Miembros, elevando así el nivel mundial de medidas contra la ciberdelincuencia y reforzando los marcos existentes.

Estructura

El Japón considera que la estructura básica que se expone a continuación sería eficaz para organizar la nueva convención, pero es partidario de proceder con flexibilidad en las próximas negociaciones sobre la elaboración de una estructura más detallada:

a) Definiciones de términos.

b) Lista de las medidas internas que deberían adoptar los Estados Miembros.

i) Tipificación:

a. actos tipificados como delitos basados en la cibernética;

b. actos que deberían tipificarse como delitos facilitados por la cibernética.

ii) Disposiciones de procedimiento relativas a la conservación, divulgación y producción de datos.

iii) Salvaguardias para garantizar el respeto de los derechos humanos y otros intereses.

c) Cooperación internacional en materia de extradición, asistencia recíproca y otras formas de cooperación.

d) Disposiciones finales.

Jordania

[Original: árabe]
[28 de octubre de 2021]

Ámbito de aplicación

La convención debería abarcar delitos relacionados con:

- la confidencialidad, la integridad y la disponibilidad de los servicios electrónicos;
- el acceso no autorizado a una red o un sistema de información o a cualquier parte de ellos;
- la perturbación de infraestructuras críticas;
- la intención de sabotear redes o sistemas de información;
- el acto de espiar el flujo de datos en una red o sistema de información;
- el fraude, la falsificación y la suplantación de identidad;
- la interceptación de datos o información de sistemas financieros;
- la violación de la privacidad y de la propiedad intelectual;
- el *hardware*, los programas informáticos de descifrado y los códigos de acceso;
- el fraude en las direcciones de Internet;
- la pornografía;
- la explotación y el abuso de niños;
- la difusión de noticias falsas;
- la discriminación racial;
- la explotación y el abuso de mujeres;
- la sedición y la incitación al discurso de odio o su difusión;
- el tráfico ilícito a través de redes de información o sitios web;
- la difusión, el apoyo o la promoción de una ideología terrorista;
- el uso de las TIC con fines terroristas;
- el acto de insultar a religiones, países y símbolos;
- las cadenas de suministro;
- los programas secuestradores;
- el *phishing* electrónico;

- la piratería informática;
- el uso no autorizado de datos por proveedores de servicios.

Objetivos

Los objetivos de la convención deberían ser:

- Reforzar la cooperación y la coordinación internacionales para combatir la utilización de las TIC con fines delictivos.
- Elaborar una legislación internacional para combatir la utilización de las TIC con fines delictivos.
- Realzar la importancia de proteger las infraestructuras críticas combatiendo la utilización de las TIC con fines delictivos.
- Promover la importancia de crear capacidad nacional e internacional y mejorar la existente, así como aumentar la concienciación de las personas y la sociedad respecto de la lucha contra la utilización de las TIC con fines delictivos.

Estructura

- Introducción.
- Definiciones.
- Objetivos.
- Ámbito de aplicación.
- Obligaciones y responsabilidades.
- Cooperación internacional.
- Creación de capacidad y sensibilización.
- Mecanismo de aplicación.
- Actualización continua de la convención para adaptarla a nuevas situaciones.

La convención debería ser de alcance amplio y abarcar el mayor número posible de países, centrándose en los que sean importantes incubadores de tecnología.

Debería incorporar conceptos internacionales acordados relativos a los delitos informáticos que afecten a personas o fondos.

La atención debería centrarse en crear medios para que los organismos de aplicación de la ley de los Estados partes intercambien información, así como mecanismos para localizar los fondos que sean el producto de delitos de fraude electrónico y descubrir la identidad digital de sus autores, conforme a la legislación nacional y respetando la privacidad.

Deberían establecerse puntos de contacto permanentes entre los Estados partes, a fin de reaccionar enseguida ante casos de terrorismo o de explotación sexual de niños, entre otros. Además, es preciso crear mecanismos para promover la cooperación con las empresas internacionales de medios sociales a fin de obtener la información técnica necesaria para reprimir ese tipo de delitos.

Debería promoverse la cooperación internacional para fomentar, mediante cursos de formación, talleres y actividades de intercambio de experiencias, la capacidad del personal de las dependencias de lucha contra el delito cibernético de los Estados partes.

Kuwait

[Original: árabe]
[17 de septiembre de 2021]

1. En la presentación general del proyecto de convención se debería subrayar que la finalidad de ese instrumento es mejorar y estrechar la cooperación para contrarrestar y reducir el riesgo de delitos relacionados con la tecnología de la información, sobre la base de la igualdad soberana de los Estados y la no injerencia en sus asuntos internos, incluidos los procedimientos relativos al ejercicio de la jurisdicción, el respeto del estado de derecho, la preservación del orden público y la seguridad y el respeto de los valores sociales.

2. Al decidir el ámbito de aplicación de la convención se deberían tener presentes los instrumentos internacionales de prevención del terrorismo, así como la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y sus protocolos, a fin de incorporar los delitos cometidos en más de un país, los preparados, planificados, dirigidos o supervisados en otros países, los cometidos en otros países o los cometidos en un país pero con consecuencias graves en otro.

3. Los actos que se tipifiquen como delito en la convención deberían determinarse de conformidad con las nuevas formas de delitos relacionados con las TIC que se definan como delitos determinantes en la legislación interna de los Estados partes, con especial atención a los delitos relativos al contenido, la incitación al odio y la violencia.

4. Deberían establecerse marcos para lo siguiente: la cooperación jurídica y judicial; la extradición de delincuentes; el intercambio de información; la permisibilidad de comunicar información sin solicitud previa si el Estado parte considera que divulgarla podría facilitar el inicio de investigaciones de esos delitos; la cooperación para compartir información de forma urgente y la preservación de información almacenada mediante tecnología de la información; el acceso a tecnología transfronteriza de la información; la cooperación y la asistencia bilaterales para reunir datos de tráfico en tiempo real; los elementos relativos a la confidencialidad; y las limitaciones para el uso de datos en el marco de la prestación de asistencia recíproca.

5. También se deberían crear marcos para evaluar la aplicación de la convención con arreglo a los mecanismos que aplicaran los Estados partes. Sería preciso designar las instituciones y los puntos de contacto pertinentes en los Estados partes, y aprovechar en lo posible las redes de información existentes de la Oficina de las Naciones Unidas contra la Droga y el Delito.

Liechtenstein

[Original: inglés]
[28 de octubre de 2021]

Liechtenstein agradece a la secretaría del Comité Especial encargado de Elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos y a su Presidenta, Excma. Sra. Faouzia Boumaiza, que haya solicitado las opiniones de los Estados Miembros sobre el ámbito de aplicación, los objetivos y la estructura (los elementos) de la nueva convención. La postura general de Liechtenstein es la que se expone a continuación.

Uno de los objetivos principales de Liechtenstein es garantizar que la nueva convención sobre la ciberdelincuencia esté en consonancia con los instrumentos internacionales y regionales existentes, como la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y el Convenio del Consejo de Europa sobre la Ciberdelincuencia, y se base en el derecho internacional, en particular las normas de derechos humanos.

Por ello, Liechtenstein aspira a que se elabore un instrumento breve y funcional, centrado expresamente en los delitos que afectan al ciberespacio, como el acceso ilícito, la interceptación ilícita, la interferencia en datos y sistemas, el uso indebido de dispositivos, la falsificación y el fraude informáticos, y los delitos relacionados con la violación de los derechos de propiedad intelectual y la utilización de niños en la pornografía. La tipificación amplia de otros tipos de delitos más allá del ámbito de los que se cometan específicamente en el ciberespacio debería contemplarse en otros instrumentos y foros, y por ello debería rechazarse. Además, Liechtenstein se opone a que se duplique la tipificación de delitos que son materia de otros tratados específicos.

Habida cuenta de que el ciberespacio es un ámbito que cambia rápidamente, Liechtenstein procurará que el lenguaje que se use en el texto de la convención sea tecnológicamente neutro para que los tipos penales sustantivos puedan aplicarse tanto a las tecnologías actuales como a las futuras. Es posible que si se utilizan definiciones técnicas extensas de tipos concretos de delitos cibernéticos queden obsoletas en el futuro, y por ello deberían evitarse en la convención.

Otro aspecto fundamental para Liechtenstein es el de las disposiciones sobre la protección de datos y los derechos humanos, a las que debería asignarse una gran importancia en la convención. Es primordial que se respeten plenamente las normas sobre la protección de datos y las normas de derechos humanos.

Liechtenstein presentará una postura más detallada durante las negociaciones de la nueva convención sobre la ciberdelincuencia.

México

[Original: español]
[21 de octubre de 2021]

Para el Gobierno de México las tecnologías de la información y telecomunicaciones, las plataformas digitales y el entorno cibernético ofrecen grandes oportunidades para potenciar el desarrollo, cerrar brechas de desigualdad, promover la inclusión, el bienestar, la justicia y los derechos.

Al mismo tiempo, México reconoce que la comisión de delitos y la propagación de un mercado ilícito mediante estas tecnologías representan una preocupación creciente para gobiernos, empresas, organizaciones sociales y todas las personas.

La cooperación internacional y los mecanismos de asistencia jurídica e intercambio de información son más necesarios que nunca. México apuesta por el multilateralismo, y en especial por el papel de las Naciones Unidas, para generar respuestas integrales y significativas ante este reto global.

México considera que el mandato generado por la Asamblea General para la elaboración de una convención integral contra el uso de las tecnologías de la información con fines delictivos, constituye una oportunidad idónea para lograr un proceso sustantivo, comprometido, plural, incluyente y transparente, y que se alimente de las lecciones aprendidas de otros procesos de Naciones Unidas relacionados con el tema, y de otras experiencias regionales vinculadas.

A continuación, se presentan los aspectos que el Gobierno de México esperaría que marcaran el proceso de elaboración y los contenidos de la futura convención.

Enfoque, alcances y tipo de convención

La convención debe ser un instrumento jurídico vinculante integral, que contemple aspectos sustantivos y procesales, orientado a establecer bases para la cooperación

internacional y el intercambio de información, experiencias, capacidades y mejores prácticas.

Se espera que contribuya a promover estándares para mejorar la investigación, mitigación y judicialización. Se espera que, si bien la convención no excluya la posibilidad de suscribir otros instrumentos internacionales en la materia, sea referente para contar con un esquema homologado que haga más eficiente la persecución de los ciberdelitos.

Se considera que deben incorporar:

- definiciones generales, tipologías básicas y actores competentes;
- medidas procesales básicas con las que deberán contar los Estados para la adecuada investigación y persecución de los delitos cibernéticos;
- tipos penales generales que debieran ser considerados por las respectivas legislaciones nacionales;
- mecanismos de acceso a la información y de fomento a la colaboración operativa.

También se considera conveniente que la futura convención permita la formulación de reservas y de declaraciones interpretativas, que contenga un procedimiento de enmienda ágil para facilitar su actualización y que establezca mecanismos para dirimir controversias. Será conveniente que la entrada en vigor se supedite al depósito de 50 instrumentos de ratificación.

Con la certeza del contenido de la convención, será oportuno acordar un mecanismo eficiente de examen de la implementación, universal, entre pares y no oneroso.

Relevancia de otros instrumentos internacionales

Para el Gobierno de México es importante que la convención parta de la afirmación de que el derecho internacional es aplicable al ciberespacio, y que por ello se tomen en consideración desarrollos existentes en diversos instrumentos jurídicos internacionales, tales como:

- la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y sus tres Protocolos complementarios;
- el Estatuto de la Corte Internacional de Justicia;
- el Convenio contra la Ciberdelincuencia del Consejo de Europa;
- tratados sobre protección y flujo transfronterizo de datos personales;
- tratados internacionales en materia de derechos humanos, y aquellos que salvaguardan las garantías de las personas que intervienen en procesos jurisdiccionales;
- tratados aplicables a la propiedad intelectual;
- tratados bilaterales en materia de extradición, asistencia jurídica mutua en materia penal y otras formas de cooperación jurídica internacional.

Se valora también que para el proceso de negociación sirvan de guía documentos adoptados en el seno de las Naciones Unidas y otros foros internacionales relevantes, principalmente:

- la recopilación de conclusiones y recomendaciones surgidas de las reuniones del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético de 2018, 2019 y 2020;

- el informe final del Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional de 2019-2021, y los informes previos de 2013 y 2015;
- el informe final del Grupo de Trabajo de Composición Abierta sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional de 2019-2021;
- el proyecto de directrices para la utilización de la Agenda sobre Ciberseguridad Global que elaboró la Unión Internacional de Telecomunicaciones (UIT);
- resoluciones de la Asamblea General de las Naciones Unidas sobre el derecho a la privacidad en la era digital;
- resoluciones del Consejo de Derechos Humanos sobre la promoción, protección y disfrute de los derechos humanos en Internet.

Delitos cibernéticos/conductas delictivas que debieran ser abordados

Para el Gobierno de México la convención debe enfatizar aquellas conductas reconocidas por el derecho internacional como ilícitas (en los términos previstos en otros tratados adoptados en el marco de las Naciones Unidas), que se realicen por medios electrónicos.

No se espera que la convención incluya un catálogo exhaustivo de delitos, ni que todas las tipologías se homologuen a los distintos sistemas jurídicos, pero sí es recomendable que en el proceso de elaboración se genere un diálogo como referente general para los siguientes casos:

- robo y suplantación de identidad;
- fraude y extorsión;
- Secuestro de información (*ransomware*);
- *malware* y conductas delictivas relacionados con la producción, almacenamiento, distribución, comercialización y ejecución de códigos maliciosos;
- exposición de información personal o institucional en perjuicio de sus propietarios;
- delitos relacionados con tráfico y trata de personas, pornografía infantil y violaciones a la intimidad sexual;
- *grooming* y acoso cibernético;
- violencia digital, incluyendo de género y por motivos de odio, racial, de nacionalidad, religión u hostilidad política;
- vectores de ataque (*phishing*, *vishing*, *smishing*, *pharming*);
- delitos contra la soberanía nacional, tales como terrorismo, sabotaje, espionaje e intrusión en los sistemas con información reservada por motivos de seguridad nacional;
- actos delictivos contra infraestructuras críticas de información y contra la confidencialidad, integridad y disponibilidad de la información;
- delitos en contra de niños, niñas y adolescentes;
- violación de la libertad de expresión;
- delitos cometidos contra la propiedad intelectual;
- delitos contra el sistema financiero;
- venta ilegal de armas, animales, medicamentos controlados y aquellos que no cuentan con registro sanitario;

- falsificación de moneda y de documentos oficiales;
- uso de criptodivisas y de bienes de uso dual con fines delictivos;
- modificación ilegal de portales (*defacement*);
- responsabilidad de las personas jurídicas.

Se considera oportuno que se discuta también, al elaborar la convención, si se admitirá la sanción a la realización de delitos en grado de tentativa, así como de determinantes que agraven el acto delictivo e incrementen las penas.

Aspectos relacionados con la soberanía y jurisdicción

- Reafirmar el respeto a la soberanía nacional y el principio de no intervención en los asuntos internos de cada Estado.
- Establecer reglas generales para la determinación de la jurisdicción aplicable, tomando como referente disposiciones similares de otros instrumentos jurídicos y procesos.
- Generar medidas comunes para la obtención de datos de tráfico y de contenido, y que prevengan la intercepción o bloqueo ilegal de datos.
- Avanzar mecanismos que den certeza a la obtención y conservación o preservación de las evidencias digitales, así como de su entrega.
- Aclarar diligencias de investigación como citaciones o aprehensiones.
- Elaborar especificaciones para la entrega de datos técnicos y de contenido en investigaciones criminales, y para la divulgación rápida de datos informáticos.
- Abordar la obligación legal de los operadores de tecnología, prestadores de servicios y contenidos en Internet para entrega de información a las autoridades competentes durante la investigación, independientemente de su localización física.

Aspectos sobre intercambio de información y cooperación internacional

Para el Gobierno de México, la convención deberá tener como uno de sus principales propósitos generar certezas para el intercambio de información y la cooperación internacional, y establecer procesos para su ejecución eficaz. Se espera que se aborden, entre otros aspectos:

- asistencia jurídica mutua;
- extradición;
- mecanismos comunes para la solicitud, respuesta, recepción e intercambio de información para la investigación y con fines de inteligencia;
- procedimientos de control judicial que permitan una colaboración ágil y efectiva durante la investigación;
- cooperación para la realización de diligencias de investigación policial y obtención de testimonios para los procesos judiciales, considerando también el uso de las tecnologías de la información y comunicación;
- elaboración de guías, estándares, metodologías y mejores prácticas para la prevención e investigación de delitos cibernéticos;
- fomento de la colaboración entre CERT o CSIRT Nacionales para la prevención de los delitos cibernéticos;
- investigaciones coordinadas;

- recomendar un marco común mínimo para la protección de la información y la transparencia, para que a pesar de las distintas políticas que a nivel nacional tiene cada Estado, se puedan compartir datos de investigaciones y procesos judiciales;
- establecer plazos mínimos para la conservación de datos y la preservación de pruebas digitales;
- recomendar reglas y términos a los cuales habrán de sujetarse las acciones de intervención de las comunicaciones privadas y la geolocalización en tiempo real;
- establecer parámetros generales para el respeto y regulación de las políticas de privacidad;
- promover la homologación de estadísticas locales, regionales y globales.

Aspectos relacionados con protección y ejercicio de derechos humanos

Todas las medidas a instrumentar desde la futura convención deberán ser consistentes con las obligaciones contenidas en los instrumentos internacionales de derechos humanos. Se espera además que sus disposiciones sean compatibles con las normas relativas a la libertad de expresión.

El Gobierno de México espera que en el proceso de elaboración de la convención se aborden:

- conceptos y desarrollos relativos a empresas y derechos humanos;
- privilegiar la investigación, persecución y castigo de la violencia de género, y de delitos contra niñas, niños y adolescentes a través de Internet;
- promover la investigación, persecución y castigo de conductas racistas, que inciten a la violencia, exclusión o segregación de las personas;
- elementos comunes mínimos acerca de la neutralidad de la red;
- recomendar mecanismos para la protección de la información por parte de empresas de servicios de Internet.

Elementos relacionados con fortalecimiento de capacidades y asistencia técnica

El Gobierno de México considera que para la instrumentación eficaz de la futura convención, será necesario establecer disposiciones que promuevan el fortalecimiento de capacidades, tanto para la prevención como para la persecución de los delitos cibernéticos. Será conveniente:

- avanzar esfuerzos de capacitación, asistencia técnica y mejores prácticas, así como procedimientos estandarizados para realizar forensia informática y obtener evidencia digital válida;
- promover iniciativas de educación para la prevención y campañas públicas replicables de concientización;
- fomentar también la creación o fortalecimiento de CERT en sectores diversos, tales como, financiero, académico, comercial y energético;
- elaborar guías, lineamientos y recomendaciones que impulsen la adopción de mejores prácticas;
- ampliar el catálogo de capacitaciones enfocadas a distintos grupos interesados: investigadores, fiscales, jueces, diplomáticos, legisladores, y actores no estatales.

Aspectos sobre participación de actores no estatales relevantes (sociedad civil, sector privado, academia)

Para el Gobierno de México resulta conveniente que desde el proceso mismo de elaboración de la convención se busquen mecanismos para facilitar la participación y la aportación de insumos de organizaciones de la sociedad civil, sector privado, proveedores de servicios, y de la academia y centros de investigación. Será deseable que se considere:

- el posible involucramiento de estos actores en los procesos para prevenir y luchar contra los delitos cibernéticos;
- promover entornos colaborativos con CERT privados, *carriers* y empresas diversas de telecomunicaciones;
- el diálogo con la iniciativa privada que opera infraestructuras críticas de información o que están dentro de los sectores estratégicos, así como con empresas proveedoras de servicios gratuitos de Internet como correo electrónico, mensajería instantánea, microblogs y servicios de transporte en línea;
- apoyar medidas de autorregulación y conciencia social, así como promover la inclusión de los conceptos de empresas y derechos humanos.

Nigeria

[Original: inglés]
[5 de noviembre de 2021]

Nigeria considera que para reaccionar con eficacia ante las amenazas que presenta la ciberdelincuencia, y que cambian rápidamente, es urgente definir y establecer sanciones para las conductas delictivas en el ciberespacio, mejorar las sinergias en cuanto a las capacidades de vigilancia transnacional, mejorar los instrumentos procesales y reformar o intensificar la cooperación internacional, en un marco de respeto de los derechos humanos. Por ello, la elaboración de una convención de las Naciones Unidas sobre esa materia debe centrarse en este momento en la lucha contra la ciberdelincuencia, y no intentar abarcar la ciberseguridad y otros asuntos relacionados con ella, que son políticamente conflictivos y se abordan de mejor manera en otros foros de las Naciones Unidas. Es imperativo que la negociación de la nueva convención sea un proceso transparente, inclusivo y consensual, de manera de promover una amplia aceptación del instrumento resultante y su aprobación.

Ámbito de aplicación

La nueva convención sobre la ciberdelincuencia debería crear un marco jurídico e institucional para combatir esta última que contenga los siguientes elementos:

a) la tipificación de los delitos cibernéticos sustantivos: determinar y fijar sanciones para los delitos basados en la cibernética, que son aquellos cuyo objetivo son las computadoras o los datos, y algunos delitos facilitados por la cibernética, así como el blanqueo del producto de la ciberdelincuencia;

b) el otorgamiento de facultades procesales para investigar y enjuiciar los delitos cibernéticos establecidos, así como para obtener e intercambiar pruebas electrónicas de la comisión de otros delitos;

c) disposiciones o medidas que favorezcan la creación de capacidad y la asistencia técnica sostenibles;

d) disposiciones o medidas para la recuperación del producto de la ciberdelincuencia y su restitución;

e) disposiciones o medidas para mejorar la colaboración y la coordinación entre los organismos de aplicación de la ley y el sector privado;

f) disposiciones o medidas para mejorar la cooperación internacional respecto de los asuntos señalados, en particular la cooperación directa con los proveedores de servicios de Internet; y

g) disposiciones o medidas para prevenir la ciberdelincuencia y promover la sensibilización, en particular mediante la colaboración con organizaciones de la sociedad civil, el sector privado, los proveedores de servicios, el mundo académico y los centros de investigación.

Objetivos

La nueva convención debería tener los objetivos siguientes:

a) lograr una comprensión común de las bases de referencia establecidas para los delitos cibernéticos sustantivos, las facultades procesales y la cooperación internacional para combatir la ciberdelincuencia;

b) promover la tipificación de los delitos de manera tecnológicamente neutra para que las disposiciones penales sustantivas abarquen no solo las tecnologías y técnicas delictivas actuales, sino también las futuras;

c) crear organismos y capacidad para reunir, obtener e intercambiar pruebas electrónicas relativas a ciberdelitos y otros delitos, en un marco de respeto de las garantías procesales, los derechos humanos y las libertades fundamentales;

d) promover y facilitar la cooperación internacional en la lucha contra la ciberdelincuencia y eliminar los refugios seguros para los autores de ciberdelitos;

e) promover la creación de capacidad y la asistencia técnica a fin de fortalecer la capacidad de los organismos de aplicación de la ley para combatir la ciberdelincuencia, así como el uso de las capacidades institucionales existentes, como las bases de datos de la Organización Internacional de Policía Criminal (INTERPOL);

f) promover la utilización por los Estados Miembros de los instrumentos multilaterales que ya han demostrado su utilidad en la lucha contra la ciberdelincuencia, como el Convenio sobre la Ciberdelincuencia del Consejo de Europa, y los nexos con los tratados existentes de las Naciones Unidas sobre prevención del delito y justicia penal, en particular la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y la Convención de las Naciones Unidas contra la Corrupción;

g) promover procesos intergubernamentales y de múltiples interesados a nivel profesional para intercambiar información con asociados fiables, a fin de detectar tendencias y amenazas futuras relacionadas con la ciberdelincuencia, así como medidas de mitigación; y

h) crear un mecanismo parar vigilar y facilitar la aplicación efectiva de la convención, el intercambio de información y el examen de cualquier revisión o modificación futura.

Estructura

Además de un preámbulo, definiciones claras y disposiciones finales adecuadas, se considera importante que los siguientes elementos formen parte de la estructura de la nueva convención:

a) disposiciones y objetivos generales y disposiciones sobre su aplicación;

b) medidas de prevención de la ciberdelincuencia, similares a las previstas en la Convención contra la Delincuencia Organizada y en la Convención contra la Corrupción; por ejemplo, disposiciones sobre iniciativas de sensibilización y educación;

c) una exposición de los ciberdelitos sustantivos y las penas aplicables;

d) disposiciones de derecho procesal y sobre las facultades generales de investigación;

e) salvaguardias para garantizar que en las actividades de aplicación de la ley se respeten las normas internacionales de derechos humanos;

f) disposiciones sobre cooperación internacional, tanto oficial como oficiosa, en la lucha contra la ciberdelincuencia para detectar, investigar y enjuiciar delitos cibernéticos, así como para obtener pruebas electrónicas de otros delitos;

g) disposiciones sobre la creación de capacidad y la asistencia técnica para mejorar las aptitudes de los profesionales y fortalecer la capacidad para combatir la ciberdelincuencia;

h) disposiciones sobre la colaboración de los profesionales con múltiples interesados para el intercambio fiable de información y experiencias con las partes pertinentes;

i) disposiciones sobre la creación de un mecanismo para vigilar y facilitar la aplicación efectiva de la convención, el intercambio de información y el examen de toda revisión o modificación futura.

Noruega

[Original: inglés]
[3 de noviembre de 2021]

El Gobierno del Reino de Noruega se complace en responder a la invitación a los Estados Miembros para que presenten sus opiniones sobre el ámbito de aplicación, los objetivos y la estructura de la nueva convención sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, en relación con la aplicación de las resoluciones 74/247 y 75/282 de la Asamblea General. La cooperación internacional es fundamental para hacer frente a las amenazas que representa la ciberdelincuencia y que cambian constantemente, y el Gobierno de Noruega espera con interés participar en las negociaciones de una convención integral sobre esta materia.

Ámbito de aplicación

En su resolución 74/247, la Asamblea General decidió establecer un comité intergubernamental especial de expertos de composición abierta, representativo de todas las regiones, a fin de elaborar una convención internacional integral sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos. Como esa resolución se refiere claramente a las conductas delictivas, la penalización de los principales delitos cibernéticos debería ser uno de los aspectos principales de la convención.

Las cuestiones relativas a la ciberseguridad y la cibergobernanza son ajenas al mandato otorgado por la Asamblea General, por lo que no deberían ser materia de la convención. Dichos asuntos corresponden a otros foros y procesos de las Naciones Unidas. Procurar incorporar disposiciones sobre ciberseguridad y cibergobernanza dificultaría la elaboración de un instrumento que reciba amplio apoyo.

La ciberdelincuencia constituye un problema desde hace decenios, y su persistencia se debe a que los delincuentes con frecuencia se adelantan a los organismos nacionales de aplicación de la ley. La ciberdelincuencia futura no será la misma de hoy, y la revolución digital en curso ha creado una tarea gigantesca para la comunidad internacional. A ese

respecto, es de suma importancia que se procure incorporar un catálogo de delitos actualizado y moderno que no quede obsoleto.

Aunque la ciberdelincuencia evoluciona todos los días, los organismos nacionales e internacionales han logrado establecer los tipos de conducta principales, que son recurrentes. Esos delitos ya se han tipificado en muchos Estados Miembros. A ese respecto, el Gobierno del Reino de Noruega recomienda que se consideren, como mínimo, los siguientes delitos basados en la cibernética y facilitados por ella:

a) el acceso ilícito, es decir, el acto de acceder a una computadora o sistema informático sin autorización;

b) la interceptación ilícita, es decir, la interceptación ilícita en tiempo real del contenido de las comunicaciones o de los datos de tráfico relacionados con las comunicaciones;

c) la interferencia en datos o sistemas, es decir, el uso de programas maliciosos, los ataques de denegación de servicio, el uso de programas secuestradores y la eliminación o modificación de datos;

d) el abuso en la utilización de dispositivos, es decir, el tráfico o la utilización de datos de crédito, contraseñas e información personal que den acceso a los recursos;

e) los delitos en que se utilicen imágenes de abusos sexuales de niños;

f) los delitos relacionados con el fraude facilitado por la cibernética, es decir, la manipulación de sistemas o datos informáticos con fines fraudulentos, como la suplantación de identidad, el acceso ilícito a correos electrónicos de empresas y el fraude en las subastas;

g) los delitos relacionados con la violación de los derechos de propiedad intelectual y otros derechos conexos.

La convención también debería contener disposiciones sobre la tentativa de cometer un delito, la ayuda para cometerlo y la incitación a ello, la confabulación para cometerlo, el blanqueo del producto del ciberdelito y la responsabilidad de las empresas y otras personas jurídicas.

Como la ciberdelincuencia evoluciona continuamente, es importante que el Comité Especial encargado de Elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos se centre en los informes actualizados de los organismos nacionales de aplicación de la ley y en los informes equivalentes de organizaciones regionales e internacionales. También es importante el Estudio Exhaustivo sobre el Problema del Delito Cibernético de la Oficina de las Naciones Unidas contra la Droga y el Delito. Además, el Gobierno del Reino de Noruega señala a la atención la *Internet Organised Crime Threat Assessment* (evaluación de la amenaza de la delincuencia organizada en Internet), publicación anual de la Agencia de la Unión Europea para la Cooperación Policial (Europol) y fuente importante de información sobre los tipos de ciberdelincuencia predominantes.

Junto con disposiciones sobre criminalización, la convención debería contener disposiciones sobre las facultades procesales, en particular sobre la reunión y el intercambio de pruebas electrónicas. Es importante que esas disposiciones sean compatibles con las garantías procesales y la protección de los derechos humanos y las libertades fundamentales.

Para hacer frente al problema de la ciberdelincuencia moderna, la convención debería exigir a los Estados Miembros que adopten disposiciones nacionales expresas sobre las pruebas electrónicas, como normas sobre la conservación rápida de los datos informáticos almacenados, el registro y la incautación de datos informáticos almacenados y la reunión en tiempo real de datos de tráfico informático y contenidos en casos de delitos graves. Además, debería prever la cooperación para obtener y reunir pruebas electrónicas relativas no solo a delitos cibernéticos, sino a cualquier tipo de delitos.

En particular, el Comité Especial debería considerar disposiciones sobre la obtención de pruebas electrónicas en la llamada “nube”. En el último decenio, el almacenamiento de datos informáticos en la nube ha sido un problema recurrente para los organismos nacionales de aplicación de la ley, debido en particular a cuestiones de jurisdicción y a la dependencia de otros Estados. Por ello, una convención moderna y actualizada sobre la ciberdelincuencia debería referirse al modo en que los Estados Miembros pueden cooperar para obtener pruebas almacenadas en la nube en otros Estados.

También es preciso que la convención contenga disposiciones sobre cooperación internacional. A ese respecto, el Comité Especial debería aprovechar la experiencia adquirida en la aplicación de los tratados existentes, en particular la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y la Convención de las Naciones Unidas contra la Corrupción. Debería considerarse la posibilidad de introducir disposiciones sobre extradición y asistencia recíproca.

También es importante que la convención refleje los distintos grados en que los Estados Miembros pueden cumplir las disposiciones propuestas, en particular las relativas a la infraestructura y las capacidades técnicas. Por ello, la convención debería prever instrumentos de creación de capacidad y establecer mecanismos para que los Estados Miembros soliciten esa asistencia.

Por último, la convención debería ocuparse de la forma en que la ciudadanía, las empresas, las organizaciones y otros interesados pueden colaborar con los Gobiernos para protegerse a sí mismos y a la comunidad de la ciberdelincuencia. Aunque la ciberseguridad no corresponde al ámbito de la convención, la prevención de la ciberdelincuencia resulta pertinente por naturaleza y debería tenerse en cuenta.

Objetivos

El Comité Especial debería procurar que se elaborara una convención sólida, que exigiera a los Estados Miembros aprobar legislación para mejorar la prevención de la ciberdelincuencia y la forma de actuar respecto a ella a nivel mundial. Serán especialmente importantes las disposiciones de derecho interno por las que se tipifiquen ciertos tipos de ciberdelincuencia, así como las relativas a las facultades procesales y la cooperación internacional.

Uno de los objetivos del proceso de redacción que se ha previsto llevar a cabo debería ser elaborar un instrumento que no se haga obsoleto y se mantenga al día respecto de todas las formas modernas de ciberdelincuencia, así como de las tendencias futuras más probables. Otro objetivo debería ser el de redactar un instrumento ambicioso, que pueda hacer frente con eficacia a los problemas principales de la ciberdelincuencia. Al mismo tiempo, es decisivo adoptar un enfoque basado en el consenso.

Además, el Gobierno del Reino de Noruega reitera la importancia de mantener un proceso abierto, inclusivo y transparente en el que participen múltiples interesados, y que permita a los Estados Miembros negociar de buena fe soluciones prácticas y bien fundamentadas, lo que a nuestro juicio es decisivo para lograr una adhesión generalizada a la nueva convención.

Estructura

Teniendo presentes el ámbito de aplicación y los objetivos propuestos de la convención, las principales partes de su estructura resultan evidentes. Sin embargo, sería útil que el Comité Especial y los Estados Miembros procedieran con flexibilidad para fijar la estructura de la convención. Aunque las disposiciones sobre tipificación, facultades procesales y cooperación internacional deberían ser los aspectos principales de la convención, hay otros asuntos que también pueden incidir en la estructura definitiva.

El Gobierno del Reino de Noruega recomienda aplicar un enfoque abierto para establecer la estructura de la convención.

Derechos humanos

Las normas internacionales de derechos humanos se aplican a las actividades cibernéticas como a cualquier otra actividad. Al igual que en el mundo físico, los Estados deben cumplir sus obligaciones en materia de derechos humanos en el ciberespacio. Los Estados deben respetar y proteger los derechos humanos, como el derecho a la libertad de expresión y el derecho a la intimidad, así como otros principios pertinentes relativos a la protección de los datos.

Es evidente que las normas de derechos humanos consagradas en el Pacto Internacional de Derechos Civiles y Políticos establecen un marco importante para todo tipo de disposiciones nuevas sobre la ciberdelincuencia. No obstante, el Gobierno del Reino de Noruega reitera la importancia de tener presentes los derechos humanos en las próximas negociaciones, en particular por lo que atañe a las disposiciones que requerirán que se elaboren leyes nacionales sobre las facultades procesales.

Nueva Zelandia

[Original: inglés]
[29 de octubre de 2021]

Nueva Zelandia se complace en responder a la invitación formulada a los Estados Miembros por la Presidenta del Comité Especial encargado de Elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos para que presenten sus opiniones sobre el ámbito de aplicación, los objetivos y la estructura de la nueva convención, por lo que atañe a la aplicación de las resoluciones 74/247 y 75/282 de la Asamblea General. Agradece la oportunidad de dar a conocer sus puntos de vista y espera con interés las contribuciones de los demás y las deliberaciones sobre la labor futura, mientras colaboramos de forma transparente e inclusiva para redactar una nueva convención.

La ciberdelincuencia es un problema transfronterizo. Por ello, para la comunidad internacional la única forma de combatir efectivamente esa amenaza cada vez más grave es la cooperación mundial basada en un enfoque inclusivo y con la participación de múltiples interesados. La cooperación internacional en asuntos relativos a la ciberdelincuencia requiere una legislación coherente y eficaz que posibilite la investigación y el enjuiciamiento transfronterizos de los delitos cibernéticos. Nunca había sido tan importante facilitar esa cooperación. Como el trabajo, la investigación y la interacción social han pasado a realizarse en línea, en particular durante la pandemia de enfermedad por coronavirus (COVID-19), han aumentado las oportunidades para los ciberdelincuentes, así como la frecuencia y la gravedad de sus actividades.

La cooperación internacional contra la ciberdelincuencia es especialmente importante para los pequeños Estados insulares en desarrollo y resulta imperativo que esos países puedan participar de manera fructífera en la labor del Comité Especial. Nueva Zelandia está comprometida a garantizar que los países insulares del Pacífico participen de manera fructífera en la labor del Comité Especial. Somos partidarios de utilizar un formato híbrido (de participación presencial y en línea) para los períodos de sesiones del Comité Especial, y subrayamos la importancia de dar tiempo suficiente a las delegaciones más pequeñas para preparar su participación.

Ámbito de aplicación

La nueva convención sobre la ciberdelincuencia debe complementar los instrumentos existentes, en lugar de contraponerse a ellos. Todos los Estados Miembros han convenido en que el derecho internacional es aplicable al ciberespacio, lo cual significa que esta nueva convención no existirá en el vacío. Su eficacia será mayor si complementa y refuerza los instrumentos existentes y el régimen jurídico actual, que comprende instrumentos que sirven para combatir la ciberdelincuencia, como la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y el Convenio sobre la Ciberdelincuencia del Consejo de Europa. Ello se ajusta al mandato establecido en la resolución 74/247 de la Asamblea General, en que la Asamblea solicitó que en la labor del Comité Especial se tuvieran plenamente en cuenta los instrumentos internacionales y las iniciativas existentes en los planos nacional, regional e internacional.

Para Nueva Zelandia es indispensable que todo instrumento que se elabore proteja los derechos humanos y favorezca la existencia de un ciberespacio libre y abierto en el que operen múltiples interesados. Por ello, la convención sobre la ciberdelincuencia debe ser compatible con las obligaciones de los Estados de proteger y respetar los derechos humanos en línea, en particular el derecho a la libertad de expresión y el derecho a no sufrir injerencias arbitrarias e ilícitas en la vida privada. Las medidas para combatir la ciberdelincuencia deben ser compatibles con las normas internacionales de derechos humanos.

El tratado debería centrarse claramente en los problemas centrales de la ciberdelincuencia, a fin de reforzar efectivamente la cooperación para hacer frente a la amenaza que esos problemas suponen para las personas, la industria y los Gobiernos. Consideramos que el tratado debería abarcar los delitos basados en la cibernética, junto con los facilitados por ella, solo en los casos en que el alcance del delito, la rapidez con que se comete y su escala aumenten por el uso de tecnologías de la información y las comunicaciones. A nuestro juicio, los dos delitos que corresponden claramente a esta categoría son, por una parte, la explotación y el abuso sexuales de niños en línea, y por la otra el fraude y el robo facilitados por la cibernética, entre otras cosas, por medio de programas secuestradores.

Nueva Zelandia no cree necesario volver a incorporar delitos ya previstos en otros instrumentos jurídicos, como la corrupción, el tráfico o el terrorismo, por el mero hecho de que estos puedan cometerse utilizando tecnologías de la información y las comunicaciones. Hacerlo entrañaría el riesgo de introducir contradicciones y confusión, y no reportaría un instrumento preciso y práctico que pudiera aumentar nuestra capacidad colectiva para combatir la ciberdelincuencia.

En el mandato establecido para este proceso se señala claramente que debemos centrarnos en elaborar un instrumento de justicia penal orientado a mejorar la reacción internacional ante la ciberdelincuencia mediante la intervención de los organismos nacionales de aplicación de la ley. Para ello se requiere definir y sancionar las conductas delictivas en el ciberespacio y que los Estados apliquen procesos e instrumentos legislativos apropiados que permitan a esos organismos obtener pruebas digitales e intercambiarlas, a fin de reprimir las conductas delictivas en el ciberespacio y sancionarlas. No se requiere definir normas de comportamiento no delictivo en línea. Consideramos que sería útil extraer lecciones de otros tratados de justicia penal que han resultado eficaces cuando se han centrado en cuestiones penales fundamentales, así como de las disposiciones amplias en materia de cooperación internacional y apoyo para crear capacidad en los Estados Miembros.

El lenguaje de la convención que se elabore debe ser práctico, tecnológicamente neutro y en lo posible, adaptable a los cambios que se produzcan en el futuro, para que no se haga obsoleto y no requiera revisión constante. Por ello, deberemos centrarnos en las actividades y no en la forma o el método concreto utilizado para realizarlas.

Sería prematuro en este momento determinar lo que puede requerirse en lo tocante al mecanismo de aplicación de la convención. Hay una gran diversidad de modelos posibles que podrían considerarse, pero este aspecto del tratado puede soslayarse hasta que se hayan definido con más claridad el ámbito de aplicación y los objetivos del instrumento.

Objetivos

El objetivo principal del nuevo instrumento debería ser establecer un marco mundial armonizado, moderno y eficaz de cooperación y coordinación entre los Estados para afrontar la amenaza cada vez más grave que supone la ciberdelincuencia para las personas, las empresas, las infraestructuras críticas y los Gobiernos. La convención debería prever la prestación de apoyo y asistencia técnica a fin de que todos los Estados desarrollen la capacidad y las aptitudes para hacer frente a esos problemas. De ese modo se aumentarían las posibilidades de los Estados de combatir eficazmente la ciberdelincuencia en los planos nacional, regional e internacional.

Ello significa que el tratado debe apoyar la cooperación entre los organismos nacionales de policía, los organismos encargados de la persecución penal y el poder judicial, de forma bilateral o multilateral, para prevenir, investigar y perseguir los delitos previstos en él. Hacerlo es fundamental para combatir la ciberdelincuencia, porque, por su naturaleza transfronteriza, los delitos cibernéticos con frecuencia tienen autores y víctimas en varias jurisdicciones. Una comprensión común de qué constituye delito en el contexto del ciberespacio y de qué delitos deberían ser punibles en las jurisdicciones nacionales facilitará cumplir ese objetivo, en particular si se complementara con marcos coherentes para obtener pruebas digitales e intercambiarlas con asociados internacionales, estableciendo las salvaguardias correspondientes.

El ejercicio de las facultades de investigación y enjuiciamiento de los delitos previstos en el tratado debe estar sujeto a salvaguardias efectivas en relación con los derechos humanos y las libertades fundamentales, como se dispone en los tratados internacionales en vigor. También debe haber salvaguardias para garantizar que los mecanismos de cooperación recíproca se utilicen de manera imparcial y adecuada, y permitan a los Estados rechazar la cooperación si no se cumplen determinadas normas. Además, Nueva Zelandia considera que el tratado debe reconocer la independencia de los organismos nacionales de policía y los organismos encargados de la persecución penal, y que toda decisión respecto de si adoptar o no medidas corresponde exclusivamente a esos organismos en los respectivos Estados Miembros.

La mejor manera de lograr una cooperación internacional eficaz es mediante un tratado que cuente con amplio apoyo. A juicio de Nueva Zelandia, ello requiere que las negociaciones relativas a ese instrumento sean inclusivas y transparentes y que se realicen todos los esfuerzos posibles por lograr un consenso, a fin de asegurar el mandato más sólido posible para la convención. Todos los Estados Miembros deberían tener la posibilidad de expresar sus opiniones, así como de participar de manera fructífera en las negociaciones, aprovechando la experiencia y las perspectivas de la sociedad civil, la industria y otros interesados. Se deberían incorporar los puntos de vista de los pueblos indígenas, como los maoríes de Aotearoa (Nueva Zelandia), y los de otras minorías, junto con sus impresiones sobre la posible repercusión de la ciberdelincuencia en dichos grupos y sus iniciativas para combatirla.

La cooperación internacional para luchar contra la ciberdelincuencia no es tan eficaz como podría serlo. Ello no se debe a la falta de voluntad de los Estados Miembros, sino a una falta de capacidad o de experiencia. La asistencia técnica y la creación de capacidad para los organismos de aplicación de la ley es un requisito fundamental, por lo que la convención debe apoyar el desarrollo de esa capacidad y de aptitudes a nivel mundial.

Estructura

Esperamos con interés recibir las opiniones de otros Estados sobre el ámbito de aplicación y los objetivos de la convención en el marco del presente proceso, así como en el primer período de sesiones destinado a las negociaciones, previsto para enero de 2022. Después de ello, prevemos que se determinará con rapidez y claridad la forma en que se procederá en relación con la estructura.

Omán

[Original: árabe]
[18 de octubre de 2021]

Se deberían tipificar como delito los ataques a instalaciones civiles, especialmente las infraestructuras vitales, como las redes de electricidad y agua, las instituciones financieras y el sector del transporte. Esas instalaciones no deberían convertirse en focos de conflicto entre países ni atacarse con el fin de ajustar cuentas.

Panamá

[Original: español]
[28 de octubre de 2021]

La constante evolución tecnológica imprime la necesidad de que los Estados adopten mecanismos para prevenir y combatir las nuevas modalidades delictivas. La pandemia de COVID-19 solo agudizó una problemática que era cada vez más evidente: no estamos suficientemente preparados para combatir la cibercriminalidad y los delitos que son ejecutados a través de medios tecnológicos.

Parte de lo que involucra estar preparados para esta batalla es tomar conciencia de que la investigación de los ciberdelitos y los delitos cometidos a través de medios informáticos no pueden divorciarse de la temática internacional. Todos los Estados nos vemos afectados por las actividades criminales de aquellos que encuentran en el transnacionalismo terreno fértil para lograr sus objetivos y evadir la responsabilidad.

Por las anteriores consideraciones, la convención internacional integral sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos debe constituirse en una herramienta que les facilite a los Estados la investigación de estos delitos. Para ello, es importante que se incluyan no solo los actos que afectan directamente a la información, los sistemas informáticos, y la tecnología en sí, sino también aquellos que, sin importar el bien jurídico protegido, son ejecutados a través de medios tecnológicos.

Consideramos que esta nueva herramienta debe adoptar medidas para perfeccionar los sistemas de comunicaciones formales e informales entre los Estados, para procurar una investigación más eficaz considerando la volatilidad de la información.

En consonancia con un sistema de comunicación más robustecido, deben tratarse ciertas figuras jurídicas que enmarcan actos de investigación como la incautación de datos y de correspondencia; la preservación de datos; y el tratamiento de la prueba electrónica.

Sabemos que pueden existir posiciones encontradas en torno a ciertos temas. Sin embargo, el objetivo sigue siendo el mismo: crear un instrumento que contribuya a la lucha contra el uso de tecnologías de la información y las comunicaciones con fines delictivos.

Reino Unido de Gran Bretaña e Irlanda del Norte

[Original: inglés]
[28 de octubre de 2021]

Ámbito de aplicación

A juicio del Reino Unido, la nueva convención internacional sobre la ciberdelincuencia debería centrarse en reforzar la cooperación para hacer frente a la creciente amenaza que supone esa actividad para ciudadanos, empresas y Gobiernos.

Hay varios tratados regionales e internacionales sobre ciberdelincuencia vigentes que ya han contribuido de manera importante a las iniciativas para combatir la ciberdelincuencia. Es importante aprovechar el éxito que han tenido esos instrumentos y reconocer las disposiciones pertinentes de los tratados de justicia penal, como la Convención de las Naciones Unidas contra la Corrupción y la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional.

El ámbito de aplicación del tratado debería abarcar: a) la investigación y el enjuiciamiento de los delitos definidos en él; b) el desarrollo de la capacidad y las aptitudes, para que todos los Estados Miembros puedan combatir esos delitos; y c) el reconocimiento de un foro de expertos cuya labor permita determinar las amenazas nuevas y emergentes.

El tratado de las Naciones Unidas sobre la ciberdelincuencia debería comprender los delitos basados en la ciberdelincuencia y los facilitados por ella, cuya escala y alcance, así como la rapidez con que se cometen, aumentan por la utilización de las computadoras. La cooperación será eficaz si en todos los ordenamientos jurídicos se entienden y reconocen del mismo modo los delitos previstos en el tratado.

La tipificación de delitos en el tratado no debería menoscabar el ejercicio de la libertad de expresión u opinión.

Este será un tratado de derecho penal y por ello debería centrarse en las actividades que han de llevar a cabo los Gobiernos. En él debería preverse también la forma en que los ciudadanos, las organizaciones no gubernamentales, las organizaciones de la sociedad civil, las instituciones académicas y el sector privado pueden colaborar, aplicando un enfoque multipartito, para protegerse de la ciberdelincuencia.

Todo tratado debe contener salvaguardias sólidas, que incluyan el respeto de la privacidad y otros derechos humanos, como se establece en las normas internacionales de derechos humanos y se reconoce en las resoluciones pertinentes de la Asamblea General y el Consejo de Derechos Humanos.

El tratado debe elaborarse de manera inclusiva y transparente, respetando las opiniones de todos los Estados Miembros y con la activa participación de una gran diversidad de interesados, entre ellas, las organizaciones no gubernamentales y de la sociedad civil, las instituciones académicas y el sector privado. Además, las disposiciones del tratado, como las relativas a la aplicación y a la creación de capacidad, deberían promover a su vez un enfoque inclusivo y transparente para la lucha contra la ciberdelincuencia.

El texto debería ser tecnológicamente neutro, para que el tratado no se haga obsoleto y no requiera que se lo actualice constantemente.

El tratado no debería repetir la labor ya realizada o que debiera realizarse en otros ámbitos. No debería abordar cuestiones de ciberseguridad, porque de ellas ya se ocupa la Primera Comisión de la Asamblea General, ni las relativas a la gobernanza de Internet, que ya son objeto de estudio de foros especializados en que participan múltiples interesados.

Objetivos

El objetivo principal del tratado debería ser apoyar la cooperación eficaz de los organismos nacionales de policía y los organismos encargados de la persecución penal, en los planos bilateral o multilateral, para la investigación y el enjuiciamiento de los delitos previstos en él. Si el instrumento recibe apoyo generalizado, favorecerá que la cooperación internacional sea lo más amplia posible.

Para apoyar una cooperación recíproca eficaz, debe preverse la posibilidad de denegarla para evitar la doble incriminación, por tratarse el delito en cuestión de un delito político —en particular si el presunto delito guarda relación con el ejercicio de la libertad de expresión— y cuando se formule una solicitud con el fin de castigar o perseguir a una persona por su raza, religión, género u otras características que justifiquen su protección. Sería útil fijar normas mínimas cuyo cumplimiento deba demostrar la autoridad requirente, por ejemplo la de que la solicitud sea necesaria y proporcionada, que respete un plazo y que haya sido autorizada por una instancia concreta.

El ejercicio de facultades para investigar y enjuiciar los delitos comprendidos en el tratado, por ejemplo, en asuntos bilaterales o multilaterales, debe estar sujeto a salvaguardias efectivas en relación con los derechos humanos y las libertades fundamentales, como se establece en las normas internacionales de derechos humanos.

El tratado debe reconocer la independencia operativa de los organismos nacionales de investigación y enjuiciamiento, y establecer que la decisión de tomar medidas corresponde exclusivamente a esos organismos.

El tratado debería apoyar el desarrollo de la capacidad a nivel mundial, y apoyar las iniciativas de creación de capacidad.

Las amenazas que suponen las actividades delictivas en el ciberespacio cambiarán, por lo que el tratado debería establecer un proceso intergubernamental y multipartito para detectar las amenazas futuras, con independencia de que dicho proceso forme parte del tratado.

Como los distintos géneros se ven afectados de manera diferente por la ciberdelincuencia, el tratado debería incorporar la perspectiva de género para contribuir a luchar contra la ciberdelincuencia más eficazmente. Elaborar un tratado sobre la ciberdelincuencia cuyas disposiciones tengan presente su repercusión en las cuestiones de género alentará a un número mayor de mujeres a participar en todos los niveles y procesos. De ese modo las soluciones serían más diversas, más ricas y, en última instancia, mejores. En la reunión del Grupo Intergubernamental de Expertos de Composición Abierta encargado de realizar un Estudio Exhaustivo del Problema del Delito Cibernético celebrada en abril de 2021, todos los Estados Miembros acordaron promover, en particular, la participación de expertas.

El tratado debería promover un enfoque de la lucha contra la ciberdelincuencia basado en la participación de toda la sociedad y alentar a los Estados Miembros a colaborar con agentes ajenos a los Gobiernos, como expertos, representantes de la industria y el público en general, respecto de asuntos como la sensibilización, la mejora de la educación, la formación en materia de género y ciberdelincuencia y el apoyo a las víctimas.

Estructura

El Reino Unido considera que la estructura que se propone a continuación sería eficaz para organizar el tratado:

a) Disposiciones generales

Las disposiciones generales deberían referirse al fundamento y la finalidad del tratado, y contener las definiciones que se utilizarán. Esas definiciones deberán reflejar una

comprensión común y ser acordadas por todas las partes, además de ser tecnológicamente neutras, para lo cual debería tenerse presente la terminología generalmente aceptada que se utiliza en los instrumentos regionales y en los marcos jurídicos nacionales.

b) Delitos básicos

Los delitos deben comprender los basados en la cibernética (por ejemplo, el acceso no autorizado), y descripciones y definiciones que sean aceptables para todas las partes. Los delitos facilitados por la cibernética (por ejemplo, la explotación y el abuso sexual de niños o el fraude) deberían incluirse si el delito se comete principalmente en línea, si el uso de computadoras modifica la escala en que se comete y la rapidez con que se perpetra y si la definición del delito se entiende comúnmente.

c) Derechos humanos y salvaguardias

La aplicación del tratado debe basarse en salvaguardias procesales efectivas y en fuertes medidas de protección de los derechos humanos, así como en las normas internacionales de derechos humanos.

d) Medidas preventivas

Al igual que la Convención contra la Corrupción y la Convención contra la Delincuencia Organizada, el tratado debería contener disposiciones que alienten a los Estados a aplicar medidas para prevenir la ciberdelincuencia, incluso mediante la colaboración con todos los interesados pertinentes.

e) Disposiciones de derecho procesal

Las facultades de apoyo a las investigaciones y el enjuiciamiento, tanto en el caso de las investigaciones internas como internacionales, deben permitir a las autoridades competentes llevar a cabo registros, incautar y conservar pruebas electrónicas de todo delito cometido por medio de una computadora o cuando las pruebas de su comisión estén en formato electrónico.

f) Cooperación internacional

Las disposiciones sobre cooperación internacional deben abarcar la asistencia judicial recíproca y la asistencia en casos de emergencia, y fijar en particular el requisito de que los países establezcan puntos de contacto permanentes. Además del intercambio práctico de pruebas, los Estados Miembros desean seguir intercambiando experiencias y mejores prácticas, así como información sobre las amenazas nuevas y de gravedad creciente, como se desprende claramente de las recomendaciones formuladas por el Grupo de Expertos en abril de 2021.

g) Asistencia técnica y creación de capacidad.

Se debería fomentar la creación de capacidad, asignando para ello una función importante a la Oficina de las Naciones Unidas contra la Droga y el Delito, y esa labor debería coordinarse a través de estructuras existentes como el Foro Mundial de Competencia Cibernética. El Reino Unido observa el gran número de recomendaciones acordadas por el Grupo de Expertos en abril de 2021 que se centran en la creación de capacidad, en particular la formación especializada y actualizada para los profesionales sobre la investigación de delitos cibernéticos, la gestión de pruebas electrónicas, la cadena de custodia y el análisis forense;

h) Aplicación

Debería establecerse un plan claro para la aplicación del tratado.

República Dominicana

[Original: español]
[5 de noviembre de 2021]

La República Dominicana saluda la oportunidad de contribuir a este ejercicio colectivo con el conjunto de los Estados Miembros con miras a presentar comentarios sobre el alcance, objetivos y estructura de un nuevo instrumento internacional sobre delito cibernético, de conformidad con las resoluciones de la Asamblea General 74/247 y 75/282, de 27 de diciembre de 2019 y 26 de mayo de 2021, respectivamente.

El delito cibernético es una forma emergente de la delincuencia transnacional, y uno de los de más rápido crecimiento a nivel mundial, cuyo auge está íntimamente ligado a la evolución y al exponencial desarrollo de las tecnologías de la información y comunicación (TIC), y afecta cada año a millones de ciudadanos y empresas.

Nuestra región, América Latina y el Caribe, se ha visto particularmente afectada por este fenómeno. Los países en desarrollo carecen en gran medida de las capacidades necesarias para combatir la delincuencia cibernética, lo cual tiene un impacto directo en las altas tasas de victimización registradas.

Asimismo, la reciente pandemia del COVID-19 puso de manifiesto las vulnerabilidades de la comunidad internacional en materia de delincuencia cibernética, lo que reafirma la importancia de una respuesta global sustentada en la colaboración y coordinación, no solo entre Estados Miembros, sino también entre los Gobiernos y las organizaciones no gubernamentales, la sociedad civil, la academia y el sector privado, toda vez que la complejidad y el alcance de la delincuencia cibernética suponen que cualquier tipo de respuesta esté fundamentada en un enfoque multidisciplinario si se quiere que la misma sea efectiva.

La República Dominicana se une con entusiasmo a este esfuerzo de la comunidad internacional y reitera su voluntad de trabajar en conjunto con todos los Estados Miembros para lograr un tratado internacional que represente a todos y cada uno de nosotros, orientado, en todo momento, por los principios de transparencia, imparcialidad e inclusión.

Ámbito de aplicación

La República Dominicana es del parecer de que el propósito central de un nuevo instrumento internacional en materia de delito cibernético es el de contar con una herramienta efectiva para la prevención, detección, investigación y persecución penal de la ciberdelincuencia, con total apego al respeto de la vida privada, la protección de datos, las libertades civiles y los derechos humanos.

De manera particular, este instrumento internacional deberá facilitar los procesos de las investigaciones criminales, permitiendo la obtención oportuna y el posterior uso de evidencia digital, reduciendo así la impunidad de ese tipo de delitos, siendo esta una de las principales limitantes que enfrentan los funcionarios encargados de hacer cumplir la ley sobre el terreno.

Asimismo, este nuevo instrumento deberá promover y facilitar la cooperación internacional entre los Estados Miembros y la asistencia técnica y el desarrollo de capacidades en los Estados partes que lo requieran en materia de delincuencia cibernética.

Asimismo, la República Dominicana es del parecer que debería dejarse claramente establecido que el nuevo instrumento debería limitarse al ámbito de la delincuencia cibernética, sin entrar en consideraciones relativas a la seguridad cibernética y la gobernanza de Internet, cuyas discusiones se llevan a cabo en otros foros.

Por otra parte, entendemos que deberán tomarse en consideración las disposiciones de los instrumentos internacionales y regionales existentes con la finalidad de no entrar en

contradicciones innecesarias con los sistemas jurídicos de los Estados Miembros que han hecho uso de dichos instrumentos como la base de sus legislaciones nacionales ni con el funcionamiento de dichos instrumentos. En este marco, se deberán aprovechar las experiencias adquiridas en la implementación de los mismos, identificando las fortalezas y las debilidades que pudieran ser complementadas por el nuevo instrumento internacional. De la misma forma, deberán tomarse en cuenta los esfuerzos de grupos especializados tales como el Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético.

Objetivos

Un nuevo instrumento internacional para la prevención y el combate de la delincuencia cibernética deberá, entre otras cosas:

- promover y facilitar una cooperación internacional ágil, práctica y efectiva entre los Estados partes;
- abarcar la prevención, detección, investigación y persecución penal de los delitos cibernéticos a los cuales se aplique el instrumento internacional, así como la recolección y el procesamiento de la evidencia digital de otros delitos, dotando a los Estados partes de las herramientas necesarias para hacer frente a ese tipo de delincuencia transnacional;
- delimitar de manera clara los tipos de delito a los que se aplicarían las disposiciones de la nueva convención y que deberán ser considerados actos ilícitos en los sistemas jurídicos de todos los Estados partes;
- promover y facilitar el desarrollo de capacidades en los Estados partes que lo requieran, con miras a evitar la creación de “paraísos cibernéticos”;
- promover el intercambio de buenas prácticas y lecciones aprendidas;
- definir reglas de juego claras para el establecimiento de la jurisdicción apropiada a los fines de solicitar evidencia digital a los proveedores “globales” de servicios de Internet, lo cual constituye en la actualidad uno de los mayores retos con miras a reducir la impunidad y dar respuestas a las víctimas de delitos cibernéticos;
- establecer salvaguardas claras y un régimen de consecuencias en caso de incumplimiento de las mismas;
- establecer poderes suficientes para investigar las infracciones penales previstas en el mismo, siempre tomando en cuenta el respeto a la vida privada, la protección de datos, las libertades civiles y los derechos humanos;
- dada la evolución rápida de los desarrollos tecnológicos, la convención debe tener una visión amplia y de largo plazo; en ese sentido, se deberá utilizar un lenguaje tecnológicamente neutral para asegurar que su vigencia en el tiempo no se vea afectada por la evolución tecnológica;
- establecer un enfoque multidisciplinario que permita una colaboración activa entre el sector público y el sector privado.

Estructura

- Definiciones.
- Tipos penales.
- Herramientas procesales para la investigación.
- Salvaguardas.
- Cooperación internacional.

- Acceso a la evidencia digital.
- Asistencia técnica y desarrollo de capacidades de investigación.
- Procedimientos operativos estandarizados.
- Medidas preventivas.
- Mecanismo de implementación.

Suiza

[Original: inglés]
[28 de octubre de 2021]

La tecnología de la información y las comunicaciones (TIC) ha tenido un impacto profundo en nuestra sociedad, creando posibilidades de desarrollo en los planos social, cultural y económico, pero también para actividades delictivas en el ciberespacio. Al irse digitalizando el mundo cada vez más, también va aumentando la ciberdelincuencia. En virtud de su resolución 74/247 la Asamblea General estableció un comité intergubernamental especial de expertos de composición abierta a fin de elaborar una convención internacional integral sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos. En la presente respuesta se expone la opinión de Suiza sobre los objetivos, el ámbito de aplicación y la estructura de ese instrumento.

Objetivos

A juicio de Suiza, el objetivo general de una convención de las Naciones Unidas sobre la lucha contra la utilización de las TIC con fines delictivos es proteger a los usuarios de esas tecnologías, para que puedan utilizarlas libremente y aprovechar sus ventajas. El carácter mundial y abierto de las TIC es, ciertamente, uno de los factores que contribuyen a acelerar el avance hacia el desarrollo social y económico. Así pues, el objetivo de la convención es garantizar la seguridad de los usuarios, que no debería limitar su libertad para utilizar las TIC. Los usuarios deben estar en condiciones de ejercer sus derechos humanos y libertades fundamentales en línea, aprovechando todas las posibilidades que ofrece un mundo digitalizado e inclusivo. Por ello, la convención debería constituir un nuevo avance para lograr que esas tecnologías sean libres, fiables y seguras.

Una convención de las Naciones Unidas puede ayudarnos a cumplir dicho objetivo general. Para ello, en la convención se debería adoptar un enfoque coordinado en la lucha contra la ciberdelincuencia. Dado el carácter intrínsecamente transnacional de las TIC, los autores y las víctimas de delitos cibernéticos tienden a encontrarse en varios Estados. Por ello, la cooperación internacional es decisiva para alcanzar el mayor grado posible de protección contra esos delitos. La convención debería orientarse a lograr una comprensión común de lo que constituye delito en el contexto de las TIC, así como de cuáles serían los delitos que deberían sancionarse en la legislación interna. Esa comprensión común es el primer elemento constitutivo para hacer posible cualquier tipo de cooperación. Basándose en esa comprensión común y en un vocabulario compartido, la convención debería tener el objetivo de crear el marco de una cooperación internacional eficaz para proteger a los usuarios de las TIC y obtener justicia para las víctimas de la ciberdelincuencia.

Un enfoque coordinado de la lucha contra la ciberdelincuencia a nivel mundial solo puede lograrse mediante un proceso inclusivo. Todos los Estados Miembros deberían tener la posibilidad de participar fructíferamente, así como la de presentar sus opiniones sobre la convención y examinar las de otros Estados durante las reuniones sustantivas del Comité Especial encargado de Elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos. El Comité debería esforzarse por lograr un consenso cuando ello sea posible.

La ciberdelincuencia es transnacional, pero la participación de agentes no estatales también es inherente a ella. Si queremos una convención idónea, se deben escuchar todas las opiniones durante el proceso de elaboración. Incluir a todas las partes interesadas, entre ellas representantes de organizaciones no gubernamentales pertinentes, organizaciones de la sociedad civil, instituciones académicas y el sector privado, en cada etapa coordinada de la elaboración es decisivo para garantizar que la convención cumpla sus objetivos[4].

Ámbito de aplicación

El derecho internacional se aplica al ciberespacio. La futura convención no existirá en el vacío, ni despojará de su importancia a los acuerdos internacionales anteriores. Suiza está convencida de que esta convención debe basarse en el régimen jurídico actual y reforzarlo. Debería concebirse para complementar las iniciativas que ya ha emprendido la comunidad internacional y aprovechar las sinergias para combatir eficazmente la ciberdelincuencia.

Como será un tratado de derecho penal, la convención debería basarse en el derecho penal internacional y respetarlo. Ya existen instrumentos mundiales que se ocupan del problema de la ciberdelincuencia. Junto con la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, el Convenio sobre la Ciberdelincuencia del Consejo de Europa es una norma conforme a la cual países de todo el mundo, incluida Suiza, han ido modernizando sus leyes sobre la ciberdelincuencia. También es una referencia importante para la cooperación internacional en la era de Internet. Una convención de las Naciones Unidas debería aprovechar esa experiencia. La labor del Comité Especial debería orientarse por la de otros grupos y foros, como el Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético.

La convención debe reflejar, salvaguardar y reforzar adecuadamente las normas de derechos humanos. Como la ciberdelincuencia amenaza los derechos humanos, toda iniciativa orientada a combatirla debe protegerlos y no menoscabarlos. Los derechos que tienen las personas cuando no están conectadas también deben protegerse cuando estén en línea. Las medidas que se adopten para combatir la ciberdelincuencia deben ser compatibles con las normas internacionales de derechos humanos.

Estructura

Suiza considera que atenerse a la estructura de los instrumentos de derecho penal internacional existentes que se han negociado en el contexto de las Naciones Unidas es un enfoque prometedor y eficaz para cumplir los objetivos señalados más arriba. Así pues, la convención podría estructurarse del siguiente modo:

a) disposiciones generales;

b) medidas preventivas;

c) penalización y aplicación de la ley;

d) cooperación internacional;

e) asistencia técnica e intercambio de información;

f) mecanismos de aplicación;

g) disposiciones finales.

Suiza considera que no hace falta duplicar delitos ya comprendidos en tratados específicos (por ejemplo, la corrupción, el tráfico, la trata y el terrorismo) por el mero hecho de que (también) puedan cometerse por medio de las TIC. En lugar de ello, la convención debería centrarse en los delitos que se cometen exclusivamente en el ciberespacio. Incluir

[4] Con arreglo a la resolución 75/282 de la Asamblea General, párrs. 9 y 10.

una lista amplia de delitos, aunque todos puedan cometerse mediante sistemas informáticos, entraña el riesgo de incurrir en contradicción y debería evitarse.

Debería reducirse al mínimo el número de delitos relacionados con el contenido y estos deberían evaluarse siempre en función de su valor añadido.

Suiza subraya la necesidad y la importancia de que se respeten garantías procesales que aseguren la legalidad y la imparcialidad de las actuaciones judiciales, así como los derechos de las personas afectadas, en particular por lo que atañe a la asistencia judicial recíproca, el intercambio de información y la extradición en las condiciones que fijen los Estados interesados. Debe garantizarse plenamente el derecho a la privacidad. También se debe garantizar un grado suficiente de protección de los datos personales.

Se deben considerar e introducir condiciones y salvaguardias adecuadas, en particular en lo concerniente al respeto y el fortalecimiento de los derechos humanos, incluido el principio de no discriminación.

Turquía

[Original: inglés]
[4 de noviembre de 2021]

Turquía asigna máxima importancia al uso libre, abierto y seguro de las tecnologías de la información y las comunicaciones en todo el mundo.

El desarrollo de las tecnologías de la información y las comunicaciones aumenta el riesgo de que esas tecnologías se utilicen con fines delictivos. Eliminar ese riesgo y las amenazas a la seguridad de las infraestructuras críticas y a los derechos y libertades fundamentales debería ser una de las prioridades principales de la agenda internacional. Debido al carácter transnacional del ciberespacio, el impacto de los ataques en ese ámbito puede ser mundial. Reducir ese impacto solo es posible llevando a cabo una cooperación eficaz en escala mundial.

A ese respecto, Turquía considera de suma importancia que exista una cooperación internacional eficaz para mantener la seguridad y estabilidad del ciberespacio a nivel mundial. En relación con ello, está dispuesta a apoyar al Comité Especial encargado de Elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos y contribuir a su labor. En este contexto, nos complacería presentar nuestras opiniones preliminares sobre el ámbito de aplicación, los objetivos y la estructura de la convención.

En el contexto de la convención se deberían tener en cuenta las siguientes cuestiones:

a) la creación de canales de cooperación eficaces entre los Estados;

b) la definición clara de los asuntos relacionados con el uso de las tecnologías de la información y las comunicaciones con fines delictivos;

c) la creación de canales de comunicación de emergencia entre los Estados;

d) el aumento de los recursos para obtener y reunir información sobre ciberamenazas;

e) la mejora del intercambio de información de inteligencia entre las instituciones pertinentes de los Estados;

f) el intercambio de información en casos que impliquen la utilización de las tecnologías de la información y las comunicaciones con fines delictivos;

Además, la convención debería prever medidas eficaces para impedir la comunicación interna entre delincuentes y terroristas, así como sus actividades de propaganda.

La pandemia de enfermedad por coronavirus (COVID-19) ha hecho que aumente considerablemente el uso de las telecomunicaciones a distancia; por ello, durante las negociaciones de la convención también deberíamos considerar el impacto de la pandemia en la utilización de las tecnologías de la información y las comunicaciones con fines delictivos.

Además, sería conveniente examinar, por lo que atañe al ámbito de aplicación del instrumento, la utilización segura de las tecnologías de nueva generación, como la computación en la nube, las redes 5G, las cadenas de bloques, la Internet de las cosas y la inteligencia artificial en la lucha contra la delincuencia y los ciberataques.

Unión Europea y sus Estados miembros

[Original: inglés]
[2 de noviembre de 2021]

El presente documento refleja los puntos de vista y la posición de la Unión Europea y de sus Estados miembros[5] sobre el ámbito de aplicación, los objetivos y la estructura (elementos) que se han de tener en cuenta en la elaboración de una nueva convención de las Naciones Unidas sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos y contribuir a la preparación del primer período de sesiones del Comité Especial encargado de Elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos, establecido a tal efecto de conformidad con la resolución 74/247 de la Asamblea General.

Esta contribución no prejuzga las posiciones ulteriores que la Unión Europea y sus Estados miembros puedan adoptar en el curso de futuras negociaciones sobre el ámbito de aplicación, los objetivos y la estructura de una futura convención de las Naciones Unidas.

I. Objetivos

La Unión Europea y sus Estados miembros subrayan que una futura convención de las Naciones Unidas debería servir de instrumento práctico para las autoridades policiales y judiciales en la lucha mundial contra la ciberdelincuencia, con el objetivo de añadir valor a la cooperación internacional. Como se expresa en las resoluciones 74/247 y 75/282 de la Asamblea General, una futura convención de las Naciones Unidas debería tener plenamente en cuenta el marco existente de instrumentos internacionales y regionales de probada eficacia en el ámbito de la delincuencia organizada y la ciberdelincuencia. Por lo tanto, cualquier nueva convención debería complementar y no menoscabar en modo alguno la aplicación de los instrumentos existentes o la futura adhesión de cualquier país a ellos y, en la medida de lo posible, evitar la duplicación.

Una futura convención de las Naciones Unidas debería contemplar la protección de los derechos humanos y las libertades fundamentales, tanto en línea como fuera de ella, y ser compatible con los instrumentos pertinentes en ese ámbito.

Una futura convención de las Naciones Unidas, tal y como acordó la Asamblea General en su resolución 75/282, debería tener plenamente en cuenta la labor[6] y los resultados[7] del Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético, de carácter intergubernamental y de composición abierta.

[5] Alemania, Austria, Bélgica, Bulgaria, Chequia, Chipre, Croacia, Dinamarca, Eslovaquia, Eslovenia, España, Estonia, Finlandia, Francia, Grecia, Hungría, Irlanda, Italia, Letonia, Lituania, Luxemburgo, Malta, Países Bajos, Polonia, Portugal, Rumania y Suecia.

[6] Véase www.unodc.org/unodc/cybercrime/egm-on-cybercrime.html.

[7] Véase UNODC/CCPCJ/EG.4/2021/2.

II. Ámbito de aplicación

Para ello, la Unión Europea y sus Estados miembros consideran que el ámbito de aplicación de una futura convención de las Naciones Unidas debería centrarse principalmente en el derecho penal sustantivo y el derecho procesal penal, así como en los mecanismos de cooperación conexos. También debería cumplir con las normas internacionales de derechos humanos y procurar luchar contra la ciberdelincuencia de la manera más eficaz posible y proteger así a las víctimas.

La Unión Europea y sus Estados miembros consideran que este nuevo instrumento debería definir con precisión los términos que en él se utilizan y dar preferencia a los conceptos ya acordados en los textos internacionales existentes.

La Unión Europea y sus Estados miembros recomiendan que el contenido de esta convención sea compacto y se centre en los elementos esenciales de la justicia penal, por lo que debería excluir en la medida de lo posible cualquier elemento accesorio.

Sobre la base de los principios expuestos, la Unión Europea y sus Estados miembros consideran que los siguientes elementos deberían incluirse en una futura convención de las Naciones Unidas:

1. Disposiciones sustantivas de derecho penal vinculadas a los delitos cibernéticos que deberían ser tipificados como tales por todos los Estados partes en una futura convención de las Naciones Unidas. En general, esas disposiciones deberían referirse únicamente a los delitos de alta tecnología y a los delitos basados en la cibernética, como el acceso ilegal a datos y sistemas informáticos y su interceptación o la interferencia ilícitas en ellos[8].

Las disposiciones sustantivas de derecho penal deben estar clara y estrictamente definidas y ser plenamente compatibles con las normas internacionales de derechos humanos y con un ciberespacio mundial, abierto, gratuito, estable y seguro. Disposiciones vagas que tipifiquen como delitos tipos de conductas que no estén claramente definidos en una futura convención de las Naciones Unidas o en otros instrumentos jurídicos universales correrían el riesgo de interferir indebidamente y de forma desproporcionada en los derechos humanos y las libertades fundamentales, incluido el derecho a la libertad de expresión, al tiempo que generarían inseguridad jurídica.

Las disposiciones sustantivas de derecho penal deberían, en la medida de lo posible, redactarse en un lenguaje tecnológicamente neutro para poder abarcar los progresos técnicos que se logren en el futuro[9]. Al mismo tiempo, debería fomentarse el intercambio de opiniones e información sobre los nuevos retos que planteen los nuevos avances tecnológicos.

Debe evitarse la incompatibilidad con otros convenios internacionales, en particular cuando determinados delitos, como el tráfico ilícito de armas o la distribución ilícita de estupefacientes, ya están ampliamente cubiertos por las disposiciones existentes en los convenios internacionales, de modo que la inclusión de este tipo de conductas en una convención sobre la ciberdelincuencia no añadiría ningún valor.

En general, en una futura convención de las Naciones Unidas se debería evitar establecer normas (mínimas) relativas a sanciones o penas para delitos específicos más allá de los modelos existentes, como el párrafo 1 del artículo 11 de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional.

[8] En consonancia con la recomendación 5, relativa a la tipificación, aprobada por el Grupo de Expertos encargado de Realizar un Estudio Exhaustivo sobre el Delito Cibernético en su reunión celebrada en Viena del 6 al 8 de abril de 2021 (véase UNODC/CCPCJ/EG.4/2021/2, anexo, recomendación 5).

[9] Véase UNODC/CCPCJ/EG.4/2021/2, anexo, recomendación 1 sobre legislación y marcos.

En lo que respecta a las normas referentes a la jurisdicción, una futura convención de las Naciones Unidas debería tomar como modelo el enfoque establecido en los instrumentos jurídicos existentes, como el artículo 15 de la Convención contra la Delincuencia Organizada.

2. Condiciones y salvaguardias sustantivas y procesales adecuadas para garantizar la compatibilidad con los derechos humanos y las libertades fundamentales, incluidos los principios de legalidad, necesidad y proporcionalidad de la acción policial y garantías sustantivas y procesales específicas que aseguren, en particular, el derecho a la privacidad y a la protección de los datos personales, el derecho a la libertad de expresión e información y el derecho a un juicio imparcial. Dichas garantías deberían basarse en las salvaguardias establecidas en otros instrumentos jurídicos internacionales pertinentes y tener al menos el mismo nivel.

3. Medidas procesales y disposiciones procesales penales relativas a los mecanismos de cooperación entre las partes en una futura convención de las Naciones Unidas, incluida la cooperación en las investigaciones y otros procedimientos judiciales y en la obtención de pruebas electrónicas, cuando proceda y sea pertinente, garantizando al mismo tiempo que puedan ser obtenidas, conservadas, autentificadas y utilizadas en actuaciones penales[10]. Dichas medidas y disposiciones tendrían que ser coherentes con los modelos establecidos en otros instrumentos jurídicos internacionales pertinentes y basarse en ellos, y complementarse con las garantías adecuadas, incluidas las que atañen a la cooperación en situaciones de emergencia.

4. Elementos, de conformidad con los derechos humanos, relativos a **la creación de capacidad, el intercambio de mejores prácticas y enseñanzas extraídas y la asistencia técnica**, incluido el importante papel que desempeña la Oficina de las Naciones Unidas contra la Droga y el Delito en esos ámbitos.

La Unión Europea y sus Estados miembros consideran que deben excluirse del ámbito de aplicación de una futura convención de las Naciones Unidas:

- los asuntos relacionados con la seguridad nacional o el comportamiento del Estado o que los regulan;
- las cuestiones relacionadas con las normas de gobernanza de Internet o que la regulan, que ya se tratan en el contexto de políticas y foros específicos de múltiples partes interesadas.

Por último, por ser un instrumento intergubernamental, una futura convención de las Naciones Unidas no debería imponer directamente obligaciones a las organizaciones no gubernamentales, entre ellas las del sector privado, como los proveedores de servicios de Internet.

III. Estructura

Sobre la base de lo señalado anteriormente, una futura convención de las Naciones Unidas podría incluir los capítulos siguientes:

Preámbulo (ámbito de aplicación y objetivos de una futura convención de las Naciones Unidas).

I. Tipos de delitos y definiciones precisas.

II. Normas procesales nacionales y principios fundamentales que deben respetarse, por ejemplo, los derechos humanos, incluidos los derechos a la privacidad y a la protección de los datos personales, y los principios de necesidad y proporcionalidad.

[10] *Ibid.*, recomendación 16, sobre pruebas electrónicas y justicia penal.

III. Cooperación internacional.

IV. Asistencia técnica, formación y creación de capacidad, y papel de la Oficina de las Naciones Unidas contra la Droga y el Delito al respecto.