



Asamblea General

Distr. general
16 de mayo de 2022
Español
Original: 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

Segundo período de sesiones

Viena, 30 de mayo a 10 de junio de 2022

Recopilación de las propuestas y contribuciones presentadas por los Estados Miembros respecto de las disposiciones sobre criminalización, las disposiciones generales y las disposiciones sobre las medidas procesales y la aplicación de la ley de una convención internacional integral sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos

Adición

Índice

	<i>Página</i>
V. Comunicaciones adicionales	2
Introducción	2
India	2
Jamaica (en nombre de la Comunidad del Caribe)	13
Malasia	22
Singapur	26
Uruguay	29



V. Comunicaciones adicionales

Introducción

En la presente adición figuran las comunicaciones presentadas por los Estados Miembros para el segundo 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 que fueron recibidas después del 14 de abril de 2022; las comunicaciones no se presentan organizadas en capítulos temáticos.

India

[Original: inglés]
[12 de mayo de 2022]

Información de antecedentes

1. El ciberespacio, al ser un medio complejo integrado por personas, programas informáticos, *hardware* y servicios en Internet, tiene características diferenciadas y únicas, en comparación con el espacio físico. El ciberespacio es virtual, no tiene fronteras y ofrece anonimato. En los últimos años, los medios sociales y el ecosistema móvil han surgido como algunos de los canales de comunicación públicos importantes. En los tiempos recientes, los medios sociales han sido considerados en todo el mundo como una herramienta fundamental que utilizan los delincuentes y los elementos antinacionales para cometer delitos cibernéticos. Dado que el ciberespacio no tiene fronteras, y que ofrece además la posibilidad de comunicarse instantáneamente y mantener el anonimato, las posibilidades de que se cometan delitos cibernéticos mediante la utilización de medios sociales e Internet son mayores que nunca en el país, así como en cualquier otra parte del mundo.

2. Los delitos cibernéticos también se han convertido en un problema importante, al estarse produciendo un aumento significativo del uso de dispositivos de tecnología de la información y las comunicaciones en todo el planeta. Los avances de la tecnología han hecho que los seres humanos dependan de la tecnología de la información y las comunicaciones para solventar todas sus necesidades. A diferencia de lo que ocurre con los delitos convencionales, en el caso de los delitos cibernéticos no existen las fronteras geográficas y no se conoce a los delincuentes, que son anónimos, lo que afecta a todos los interesados, entre ellos, a los ciudadanos comunes. En la siguiente sección se hace hincapié en los tipos de delitos cibernéticos que se cometen en todo el mundo.

Clasificación de los delitos que se cometen mediante la utilización de las tecnologías de la información y las comunicaciones

3. “Delitos cibernéticos” es un término amplio que se utiliza para englobar la actividad delictiva en que se utilizan computadoras o redes de computadoras como herramientas, o en que estas son el objetivo de la actividad delictiva o el ámbito en que esa actividad se desarrolla e incluyen todos los actos, desde el daño a los servicios electrónicos hasta la ejecución de ataques de denegación de servicio. En general, los delitos cibernéticos pueden clasificarse en delitos facilitados por la cibernética¹ y delitos basados en la cibernética². Además, los delitos cibernéticos pueden clasificarse en “delitos cibernéticos contra las personas”, “delitos cibernéticos contra la propiedad” y “delitos cibernéticos contra el Gobierno”. Sin embargo, tal vez sea mejor utilizar la

¹ Los robos, los acosos, la explotación de niños, los fraudes y las estafas pueden cometerse sin computadoras, pero son delitos que el uso de computadoras facilita en algunas circunstancias.

² La piratería informática, los programas secuestradores, los ataques de denegación de servicio distribuido y los programas maliciosos, la distribución de virus y el ciberterrorismo.

expresión “delitos cometidos mediante la utilización de tecnologías de la información y las comunicaciones” para comprender también las tecnologías nuevas y emergentes.

Criminalización

4. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito o como una infracción equivalente según su derecho interno las conductas que se señalan a continuación. (La lista es ilustrativa y pueden añadirse a ella otros delitos que se cometan mediante la utilización de tecnologías de la información y las comunicaciones).

4 a) Daños a una computadora, a un sistema informático, etc.

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito, de conformidad con su derecho interno, el que una persona, sin permiso de su propietario o de otra persona que se encuentre a cargo de una computadora, sistema informático o red de computadoras:

- a) acceda u obtenga acceso a esa computadora, sistema informático o red de computadoras o recurso informático;
- b) descargue, copie o extraiga datos, bases de datos informáticas o información de esa computadora, sistema informático o red de computadoras, incluida la información o los datos conservados o almacenados en cualquier dispositivo de almacenamiento informático de datos extraíble;
- c) introduzca o haga que se introduzca cualquier contaminante informático o virus informático en cualquier computadora, sistema informático o red de computadoras;
- d) dañe o haga que se dañe cualquier computadora, sistema informático o red de computadoras, datos, bases de datos informáticas o cualquier otro programa que se aloje en esa computadora, sistema informático o red de computadoras;
- e) cause una perturbación o haga que se cause una perturbación en cualquier computadora, sistema informático o red de computadoras;
- f) deniegue o haga que se deniegue el acceso a cualquier persona autorizada a acceder a cualquier computadora, sistema informático o red de computadoras, por cualquier medio;
- g) proporcione asistencia a cualquier persona para facilitar el acceso a una computadora, sistema informático o red de computadoras en contravención de las disposiciones de la presente Ley o los reglamentos que se aprueben en virtud de ella;
- h) cargue los servicios utilizados por una persona a la cuenta de otra mediante la alteración o manipulación de cualquier computadora, sistema informático o red de computadoras;
- i) destruya, borre o altere cualquier información que se aloje en un recurso informático o disminuya su valor o utilidad o lo afecte de modo que cause un daño, por cualquier medio;
- j) robe, oculte, destruya o altere, o haga que cualquier persona robe, oculte, destruya o altere, cualquier código fuente informático utilizado para un recurso informático con la intención de causar un daño.

4 b) Negligencia en la protección de datos

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno el que una persona jurídica que posea, manipule o trate información o datos personales delicados que se encuentren almacenados en un recurso informático del que sea propietaria o que controle u opere sea negligente en la implementación y mantenimiento de prácticas y procedimientos de

seguridad razonables y cause en consecuencia un daño ilegítimo a cualquier persona o genere un beneficio ilegítimo para cualquier persona.

4 c) *Alteración de documentos informáticos originales*

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno, el hecho de que cualquier persona, a sabiendas o intencionalmente, oculte, destruya o altere o, a sabiendas o intencionalmente, haga que otro oculte, destruya o altere cualquier código fuente informático utilizado para una computadora, programa informático o red de computadoras, cuando la ley exija que el código fuente informático se conserve o mantenga mientras se encuentre vigente.

4 d) *Envío de mensajes ofensivos mediante servicios de comunicaciones, etc.*

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito, de conformidad con su derecho interno, el envío por cualquier persona, mediante un recurso informático o un dispositivo para comunicaciones, de lo siguiente:

a) cualquier información que sea gravemente ofensiva o amenazadora;

b) cualquier información que quien la envía sepa es falsa, con el fin de generar molestias, inconvenientes, peligros u obstrucción, insultar, dañar, intimidar, causar enemistad, odio o mala voluntad, de forma persistente, mediante la utilización de un recurso informático o dispositivo para comunicaciones;

c) cualquier correo electrónico o mensaje de correo electrónico con el fin de generar molestias o inconvenientes, engañar o inducir a engaño a su destinatario o receptor sobre el origen del mensaje.

4 e) *Recepción deshonesto de recursos informáticos o dispositivos para comunicaciones robados*

Quien reciba o conserve deshonestamente cualquier recurso informático o dispositivo para comunicaciones robado a sabiendas de que ese recurso informático o dispositivo para comunicaciones es robado o tuviera razones para creer que ese recurso informático o dispositivo para comunicaciones es robado.

4 f) *Robo de identidad (suplantación de identidad)*

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito, de conformidad con su derecho interno, el uso fraudulento o deshonesto por cualquier persona de una firma electrónica, contraseña o cualquier otro elemento único de identificación de cualquier otra persona.

4 g) *Engaño consistente en la suplantación de identidad mediante la utilización de recursos informáticos (suplantación de identidad)*

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito, de conformidad con su derecho interno, el engaño que realice cualquier persona suplantando una identidad mediante la utilización de un dispositivo para comunicaciones o recurso informático.

4 h) *Violación de la privacidad*

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito, de conformidad con su derecho interno, la captación, publicación o transmisión, a sabiendas o intencionalmente, de la imagen de una parte privada de una persona sin el consentimiento de esta, en circunstancias que impliquen la violación de la privacidad de esa persona:

a) Por “transmitir” se entenderá enviar electrónicamente una imagen visual con la intención de que sea vista por una o más personas;

- b) Por “capturar”, en relación con una imagen, se entenderá registrar en vídeo, fotografiar, filmar o grabar por cualquier medio;
- c) Por “parte privada” se entenderán los genitales, el área púbica o las nalgas, o los senos de una persona de sexo femenino, desnudos o vestidos con ropa interior;
- d) Por “publicación” se entenderá la reproducción en forma impresa o electrónica y la puesta a disposición del público;
- e) Por “en circunstancias que impliquen la violación de la privacidad” se entenderá que en esas circunstancias la persona puede tener una expectativa razonable de que:
 - i) puede desvestirse en privado sin la preocupación de que se esté capturando una imagen de sus partes privadas, o
 - ii) que sus partes privadas no serán visibles para la sociedad, con independencia de si la persona de que se trate se encuentra en un lugar público o privado.

4 i) *Ciberterrorismo*

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito, de conformidad con su derecho interno, el que una persona:

- a) con la intención de amenazar la unidad, integridad, seguridad o soberanía del Estado o infundir terror en la población o en cualquier sector de la sociedad:
 - i) deniegue o haga que se deniegue el acceso a cualquier persona autorizada a acceder a un recurso informático; o
 - ii) intente penetrar o acceder a un recurso informático sin autorización o excediendo la autorización que tiene para el acceso, o
 - iii) introduzca o haga que se introduzca cualquier contaminante informático;

y por medio de esa conducta cause o sea probable que cause la muerte de una persona o lesiones a una persona o dañe o destruya bienes o perturbe suministros o servicios esenciales para la vida de la comunidad o afecte negativamente a infraestructuras de la información críticas, a sabiendas de que es probable que causará ese daño o perturbación, o

- b) a sabiendas o intencionalmente penetre un recurso informático o acceda a él sin autorización o excediendo su autorización de acceso y mediante esa conducta obtenga acceso a información, datos o una base de datos informática que se encuentre restringida por razones de seguridad del Estado o de sus relaciones exteriores o a cualquier información, datos o base de datos restringida, cuando tenga razones para creer que esa información, datos o base de datos informática así obtenidos podrían utilizarse para lesionar, o sea probable que lesionen, intereses relativos a la soberanía y la integridad o la seguridad del Estado, sus relaciones de amistad con Estados extranjeros, el orden público, la decencia o la moral, o cometa el delito de ciberterrorismo en relación con el desacato a una autoridad judicial, difamación o incitación a cometer un delito o para beneficiar a una nación extranjera o grupo de personas o de cualquier otro modo.

2. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito, de conformidad con su derecho interno, la comisión o la confabulación para cometer las conductas delictivas descritas en los apartados a) y b) del párrafo 1.

4 j) *Publicación o transmisión de material obsceno en comunicaciones en forma electrónica*

Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito, de conformidad con su derecho interno, la publicación o transmisión o el hacer que se publique o transmita, en forma electrónica,

cualquier material lascivo o que apele al interés lúbrico o cuyo efecto sea tal que tienda a pervertir o corromper personas que probablemente, teniendo en cuenta todas las circunstancias pertinentes, lean, vean u escuchen los asuntos contenidos o plasmados en ese material.

4 k) *Publicación o transmisión de material que muestre actos sexuales explícitos, etc., en forma electrónica*

Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito, de conformidad con su derecho interno, la publicación o transmisión en forma electrónica de cualquier material que muestre actos o conductas sexuales explícitos o el hacer que se publique o transmita ese material en forma electrónica.

4 l) *Publicación o transmisión de material que muestre niños realizando actos sexuales explícitos, etc., en forma electrónica*

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito, de conformidad con su derecho interno, el que una persona:

a) publique o transmita, o haga que se publique o transmita, en cualquier forma electrónica, material que muestre niños realizando actos o conductas sexualmente explícitas; o

b) cree texto o imágenes digitales, obtenga, procure conseguir, busque, descargue, publicite, promocióne, intercambie o distribuya material, en cualquier forma electrónica, que muestre niños de manera obscena, indecente o sexualmente explícita; o

c) persuada o induzca a niños a participar en una relación en línea, o cultive esa relación, con uno o más niños para cometer un acto sexualmente explícito o en un modo que pueda ofender a un adulto razonable en el recurso informático; o

d) facilite la comisión de abusos contra niños en línea, o

e) grabe de cualquier forma electrónica sus propios actos de abuso o los de otros relacionados con la realización de actos sexuales explícitos con niños;

siempre que lo dispuesto en la presente sección no se reproduzca en un libro, folleto, documento, escrito, dibujo, representación pictórica o figura en forma electrónica:

i) cuya publicación se encuentre justificada por servir un interés público en razón de que ese libro, folleto, documento, escrito, dibujo, representación pictórica o figura se haga en interés de la ciencia, la literatura, el arte o la educación u otros objetos de interés general, o

ii) que se conserve o se utilice de buena fe con fines religiosos o para la preservación del patrimonio cultural.

La edad de los niños será la que defina el derecho interno del Estado.

4 m) *Revelación de información en incumplimiento de un contrato legítimo*

Salvo disposición en contrario de la presente Convención, el que una persona —incluido un intermediario— que hubiera obtenido acceso a cualquier material en que figurara información personal sobre otra persona, aun cuando estuviera prestando servicios en virtud de un contrato legítimo, revelara dicho material a un tercero con intención de causar, o a sabiendas de que probablemente causará, un daño ilegítimo o con la intención de generar, o a sabiendas de que probablemente generará, un beneficio ilegítimo, sin el consentimiento de la persona de que se trate o en infracción de un contrato legítimo.

5. Otros actos ilícitos cometidos mediante la utilización de tecnologías de la información y las comunicaciones

Sin perjuicio del (artículo relativo a la protección de la soberanía) las Partes contratantes se pondrán de acuerdo en qué otros actos ilícitos cometidos mediante la utilización de tecnologías de la información y las comunicaciones a los fines de cooperación establecidos en esta Convención constituirán delito. (Debería preverse una disposición en la Convención titulada “Otros actos ilícitos” en que se consideraran los avances en las tecnologías de la información y las comunicaciones). Además, en la presente Convención, podrán ampliarse los siguientes delitos cibernéticos, como se menciona en el documento de la Oficina de las Naciones Unidas contra la Droga y el Delito³:

- acceso ilícito;
- interceptación ilícita: interceptación ilegítima, por medios técnicos, de transmisiones no públicas de datos informáticos hacia o desde un sistema informático o en él, incluidas las interferencias ilegales electromagnéticas;
- uso indebido de herramientas informáticas;
- delitos contra la identidad;
- daños personales;
- racismo y xenofobia;
- delitos relacionados con el respaldo al terrorismo;
- programas secuestradores.

13. Términos utilizados

a) Por “dispositivo para comunicaciones” se entenderán los teléfonos celulares, los servicios de asistencia digital personal o la combinación de ambos o cualquier otro dispositivo utilizado para comunicar, enviar o transmitir cualquier texto, vídeo, audio o imagen;

b) Por “computadora” se entenderá todo dispositivo o sistema de procesamiento de datos de alta velocidad electrónico, magnético, óptico o de otro tipo que realice funciones lógicas, aritméticas y de memoria mediante la manipulación de impulsos electrónicos, magnéticos u ópticos, incluido todo ingreso, salida, procesamiento y almacenamiento de datos, programas informáticos o servicios de comunicación conectados o relacionados con una computadora en un sistema o red informáticos;

c) Por “red de computadoras” se entenderá la interrelación entre una o más computadoras o sistemas informáticos o dispositivos para comunicaciones mediante:

- i) la utilización de medios de comunicación inalámbricos, por satélite, microondas o cable o líneas terrestres, u otros medios de comunicación, y
- ii) terminales o un complejo consistente en dos o más computadoras interconectadas o dispositivos para comunicaciones, sea que la interconexión se mantenga de forma continua o no;

d) Por “recursos informáticos” se entenderán las computadoras, los sistemas informáticos, las redes de computadoras, los datos, las bases de datos informáticos o los programas informáticos;

e) Por “sistema informático” se entenderá un dispositivo o conjunto de dispositivos —incluidos los dispositivos para apoyar el ingreso y egreso de datos, y excluidas las calculadoras que no sean programables o capaces de ser utilizadas con archivos externos—, que contenga programas informáticos, instrucciones electrónicas, datos de entrada y de salida, y que realice operaciones lógicas o aritméticas, de

³ Fuente: Oficina de las Naciones Unidas contra la Droga y el Delito, *Estudio exhaustivo sobre el delito cibernético*, borrador de febrero de 2013, pág. 22.

almacenamiento y recuperación de datos, de control de las comunicaciones y otras funciones;

f) Por “contaminante informático” se entenderá cualquier conjunto de instrucciones para computadora concebidas para:

i) modificar, destruir, grabar, transmitir datos o programas alojados en una computadora, un sistema informático o una red de computadoras, o

ii) de cualquier modo, usurpar el funcionamiento normal de una computadora, un sistema informático o una red de computadoras;

g) Por “base de datos informática” se entenderá una representación de información, conocimientos, hechos, conceptos o instrucciones en texto, imagen, audio o vídeo que se estén preparando o hayan sido preparados formalmente o hayan sido producidos por una computadora, un sistema informático o una red de computadoras y que estén destinados a ser utilizados en una computadora, un sistema informático o una red de computadoras;

h) Por “virus informático” se entenderán las instrucciones informáticas, informaciones, datos o programas que destruyan, dañen, degraden o afecten negativamente al funcionamiento de un recurso informático o se adhieran a otro recurso informático y que operen cuando se ejecuten programas, datos o instrucciones o cuando se produzca algún otro hecho en ese recurso informático;

i) Por “dañar” se entenderá destruir, alterar, borrar, añadir, modificar o reorganizar cualquier recurso informático por cualquier medio;

j) Por “código fuente informático” se entenderá la lista de programas, órdenes informáticas, diseños y análisis de programas de recursos informáticos en cualquier forma;

k) Por “ciberseguridad” se entenderá la protección de información, equipo, dispositivos, computadoras, recursos informáticos, dispositivos para comunicaciones e información almacenada en ellos contra el acceso, uso, revelación, perturbación, modificación o destrucción no autorizados;

l) Por “datos” se entenderá la representación de información, conocimientos, hechos, conceptos o instrucciones que se estén preparando o se hayan preparado formalmente y que se tenga la intención de procesar, se esté procesando o se haya procesado en un sistema informático o red de computadoras o nube, y que pueda encontrarse en cualquier forma (incluso impresiones de computadora, medios de almacenamiento magnéticos u ópticos, tarjetas o cintas perforadas) o se haya almacenado internamente en la memoria de la computadora;

m) “Información” incluye datos, mensajes, textos, imágenes, sonidos, voz, códigos, programas informáticos, bases de datos o microfilms o microfichas generadas por computadora;

n) Por “persona jurídica” se entenderán las sociedades comerciales, incluidas las firmas, empresas unipersonales u otras asociaciones de personas físicas que realicen actividades comerciales o profesionales;

o) Por “procedimientos y prácticas de seguridad razonables” se entenderán las prácticas y los procedimientos de seguridad orientados a proteger la información contra el acceso, daño, uso, modificación, revelación o deterioro no autorizados, según se especifique en un acuerdo entre las partes o en una ley que se encuentre vigente en ese momento y, a falta de ese acuerdo o ley, las prácticas y los procedimientos de seguridad razonables que los Estados partes, en consulta con las asociaciones u órganos profesionales que estos consideren adecuado consultar, determinen que deben establecerse;

p) Por “información o datos personales delicados” se entenderá información personal, según determinen los Estados partes, en consulta con las asociaciones u órganos profesionales que estos consideren adecuado consultar;

q) Por “correo electrónico” o “mensaje de correo electrónico” se entenderá un mensaje o información creados en o transmitidos o recibidos por una computadora, sistema informático, recurso informático o dispositivo para comunicaciones, incluidos documentos adjuntos de texto, imagen, audio, vídeo y cualquier otro documento electrónico que se transmita con el mensaje;

r) Por “intermediario de medios sociales” se entenderá un intermediario cuya principal o única función sea permitir la interacción en línea entre dos o más usuarios, facilitándoles crear, cargar, compartir, diseminar, modificar o acceder a información utilizando sus servicios;

s) Por “documentos electrónicos” se entenderán los datos o documentos generados, las imágenes o sonidos almacenados, recibidos o enviados en forma electrónica o microfilms o microfichas generadas por computadora;

t) Por “originador” se entenderá una persona, excluidos los intermediarios, que envíe, genere, almacene o transmita cualquier mensaje electrónico o haga que se envíe, genere, almacene o transmita ese mensaje electrónico a cualquier otra persona;

u) Por “bienes” se entenderán los activos de cualquier tipo, corporales o incorporales, muebles o inmuebles, tangibles o intangibles, incluido el dinero en cuentas bancarias, los activos financieros digitales, las monedas digitales, incluidas las criptomonedas y los documentos o instrumentos legales que acrediten la propiedad u otros derechos sobre dichos activos;

v) Por “producto del delito” se entenderán los bienes obtenidos o derivados, directa o indirectamente, de la comisión de un delito u otro acto ilícito tipificado de conformidad con la presente Convención;

w) Por “decomiso” se entenderá la privación con carácter definitivo de bienes por orden de un tribunal u otra autoridad competente;

x) Por “delito determinante” se entenderá todo delito del que se derive un producto que pueda pasar a constituir materia de un delito definido en la presente Convención;

y) Por “pornografía infantil” se entenderá toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales.

14. Jurisdicción fundada en los datos

La jurisdicción fundada en los datos significa que el Estado del que sea nacional la persona cuyos datos sean almacenados, procesados, examinados o federados en cualquier parte del mundo debería ser quien tuviera competencia en general sobre los datos, con independencia de dónde se almacenaran, procesaran, examinaran o federaran esos datos físicamente. La jurisdicción fundada en los datos asegurará que prevalezcan como criterios la propiedad de los datos y la privacidad (un derecho fundamental reconocido del ciudadano global), así como los derechos humanos.

(Breve explicación: en el contexto actual, la jurisdicción fundada en el modelo clásico de Westfalia no resulta útil en el ciberespacio, especialmente en lo que respecta a los recursos alojados en la nube, que pueden derivar en una pesadilla jurisdiccional. Un ejemplo de situación que sería típica es el caso de un delito cibernético para cuya ejecución se utiliza originalmente el poder de procesamiento en la nube en un país, y después la agregación de almacenamiento se produce en un segundo país; el proveedor de servicios en la nube se encuentra registrado en un tercer país, y los usuarios (la víctima y el atacante), cuyos datos retiene el proveedor de servicios, tal vez sean residentes de un cuarto. Es claro que en esa situación, resulta extremadamente difícil verificar la jurisdicción en función de modelos territoriales clásicos. En vista de lo señalado, la India propone que, más que el modelo de jurisdicción fundado en el territorio, en la Convención se adopte como criterio la jurisdicción fundada en los datos. La propiedad de los datos vinculada a la privacidad constituye un derecho fundamental reconocido del ciudadano global, lo que ha sido confirmado por el

Tribunal de Justicia de la Unión Europea, que reconoció el derecho de las personas al olvido. El derecho a la privacidad también se encuentra vinculado a los derechos humanos y ha sido planteado por un gran número de países en el Comité Especial; la jurisdicción fundada en los datos contribuirá a proteger el derecho a la privacidad, los derechos fundamentales y los derechos humanos).

15. Propuesta de definición de “jurisdicción”

1. Cada Estado parte adoptará las medidas que resulten necesarias para establecer su jurisdicción respecto de los delitos tipificados con arreglo a la presente Convención cuando:

a) el delito se cometa en el territorio de ese Estado parte o tenga relación con el territorio del Estado parte, o

b) el delito se cometa a bordo de un buque que enarbole su pabellón o de una aeronave registrada conforme a sus leyes en el momento de la comisión.

2. Con sujeción a la presente Convención, un Estado parte también podrá establecer su jurisdicción para conocer de tales delitos cuando:

a) el delito sea cometido contra uno de sus nacionales y personas jurídicas de ese Estado parte; o

b) el delito sea cometido por uno de sus nacionales o personas jurídicas de ese Estado parte o por una persona apátrida que tenga residencia habitual en su territorio; o

c) el delito sea cometido fuera de su territorio con miras a la comisión, dentro de su territorio, de un delito tipificado con arreglo a la presente Convención;

d) el delito sea cometido contra el Estado parte; o

e) el delito sea cometido contra los recursos informáticos ubicados en su territorio;

f) el delito se relacione con los datos digitales o electrónicos de sus nacionales, con independencia del lugar en que se los almacene, procese, examine o federe físicamente.

3. A los efectos de la presente Convención, cada Estado parte adoptará las medidas que resulten necesarias para establecer su jurisdicción respecto de los delitos tipificados con arreglo a la presente Convención cuando el presunto delincuente se encuentre en su territorio y el Estado parte no lo extradite por el solo hecho de ser uno de sus nacionales.

4. Cada Estado parte podrá también adoptar las medidas que resulten necesarias para establecer su jurisdicción respecto de delitos tipificados con arreglo a la presente Convención cuando el presunto delincuente se encuentre en su territorio y el Estado parte no lo extradite.

5. Si un Estado parte que ejerce su jurisdicción con arreglo a los párrafos 1 o 2 del presente artículo ha recibido notificación, o tomado conocimiento por otro conducto, de que otros Estados parte están realizando una investigación, un proceso o una actuación judicial respecto de los mismos hechos, las autoridades competentes de esos Estados partes se consultarán, según proceda, a fin de coordinar sus medidas. A los fines de las consultas que se realicen de conformidad con lo dispuesto en el presente artículo, las Partes contratantes tendrán en cuenta la jurisdicción fundada en los datos, es decir, que los datos pertenecen a la víctima del delito cibernético o acto ilícito cometido mediante la utilización de tecnologías de la información y las comunicaciones.

6. Sin perjuicio de las normas del derecho internacional general, la presente Convención no excluirá el ejercicio de las competencias penales establecidas por los Estados parte de conformidad con su derecho interno.

17. Registro e incautación de información almacenada o procesada electrónicamente

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para facultar a sus autoridades competentes a registrar o acceder de un modo similar:

a) a todo sistema informático o a parte de él, así como a los datos informáticos en él almacenados, y

b) a todo dispositivo de almacenamiento informático que permita almacenar datos informáticos en su territorio.

2. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para asegurarse de que cuando de conformidad con el párrafo 1 a) sus autoridades registren o tengan acceso de un modo similar a un sistema informático específico o a una parte de él y tengan motivos para creer que los datos buscados se hallan almacenados en otro sistema informático o en una parte de él situado en su territorio, y que dichos datos son legítimamente accesibles a partir del sistema inicial o están disponibles por medio de dicho sistema inicial, puedan extender rápidamente el registro o el acceso que hayan tenido de un modo similar al otro sistema.

3. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para facultar a sus autoridades competentes a incautar o a obtener de un modo similar los datos informáticos a los que se haya accedido en aplicación de los párrafos 1 o 2. Estas medidas incluirán las siguientes prerrogativas:

a) incautar u obtener de un modo similar un sistema informático o una parte de él, o un dispositivo de almacenamiento informático;

b) realizar y conservar una copia de esos datos informáticos;

c) preservar y mantener la integridad de los datos informáticos.

4. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para facultar a sus autoridades competentes a ordenar a toda persona que conozca el funcionamiento de un sistema informático o las medidas aplicadas para proteger los datos informáticos que este contenga, que proporcione toda la información necesaria, dentro de lo razonable, para permitir la aplicación de las medidas previstas en los párrafos 1 y 2.

18. Obtención en tiempo real de datos relativos al tráfico

1. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para facultar a sus autoridades competentes:

a) a obtener o grabar con medios técnicos existentes en su territorio, y

b) a obligar a cualquier proveedor de servicios, en la medida de sus capacidades técnicas:

i) a obtener o grabar con medios técnicos existentes en su territorio, o

ii) a prestar a las autoridades competentes su colaboración y su asistencia para obtener o grabar en tiempo real los datos relativos al tráfico asociados a comunicaciones específicas transmitidas en su territorio por medio de un sistema informático.

2. Cuando una Parte no pueda adoptar las medidas enunciadas en el párrafo 1 a) en razón de los principios establecidos en su ordenamiento jurídico interno, podrá, en su lugar, adoptar las medidas legislativas y de otra índole que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos relativos al tráfico asociados a comunicaciones específicas transmitidas en su territorio mediante la aplicación de medios técnicos existentes en dicho territorio.

3. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el que se haya

ejercido cualquiera de las facultades previstas en el presente artículo, así como toda información al respecto.

19. Obtención de contenido y metadatos

1. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para proporcionar metadatos rápidamente sin necesidad de que se firmen tratados de asistencia judicial recíproca. El proveedor de servicios que posea esos metadatos proporcionará esa información en respuesta a la solicitud directa que hagan las autoridades encargadas de la aplicación de la ley por conducto de un enlace que se designará en cada Estado.

2. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para proporcionar datos de contenido rápidamente. El mecanismo para ese intercambio de datos rápido se elaborará de conformidad con la presente Convención.

20. Interceptación de datos relativos al contenido

1. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para facultar a sus autoridades competentes en lo que respecta a un repertorio de delitos graves que deberá definirse en su derecho interno:

- a) a obtener o grabar con medios técnicos existentes en su territorio, y
- b) a obligar a cualquier proveedor de servicios, en la medida de sus capacidades técnicas:
 - i) a obtener o grabar con medios técnicos existentes en su territorio, o
 - ii) a prestar a las autoridades competentes su colaboración y su asistencia para obtener o grabar en tiempo real los datos relativos al contenido de comunicaciones específicas transmitidas en su territorio por medio de un sistema informático.

2. Cuando una Parte no pueda adoptar las medidas enunciadas en el párrafo 1 a) en razón de los principios establecidos en su ordenamiento jurídico interno, podrá, en su lugar, adoptar las medidas legislativas y de otra índole que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos relativos al contenido asociados a comunicaciones específicas transmitidas en su territorio mediante la aplicación de medios técnicos existentes en dicho territorio.

3. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se haya ejercido cualquiera de los poderes previstos en el presente artículo, así como toda información al respecto.

21. Conservación rápida de datos informáticos almacenados

1. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para permitir a sus autoridades competentes ordenar o imponer de otro modo la conservación rápida de datos electrónicos específicos, incluidos los datos relativos al tráfico y contenido, almacenados por medio de un sistema informático, en particular cuando existan motivos para creer que dichos datos son particularmente susceptibles de pérdida o de modificación.

2. Cuando una Parte aplique lo dispuesto en el párrafo 1 anterior por medio de una orden impartida a una persona de que conserve determinados datos almacenados que se encuentren en poder o bajo el control de esa persona, la Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para obligar a dicha persona a conservar y a proteger la integridad de los datos durante el tiempo necesario, hasta un máximo de 180 días, con el fin de que las autoridades competentes puedan lograr que se los revele. Las Partes podrán prever que dicha orden pueda renovarse.

3. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para obligar a la persona que custodie los datos o a otra persona encargada

de su conservación a mantener en secreto la ejecución de dichos procedimientos durante el tiempo previsto en su derecho interno.

4. Cada Parte establecerá un enlace para la coordinación, por cuyo conducto el otro Estado cumplirá la solicitud de conservación.

Jamaica (en nombre de la Comunidad del Caribe)

[Original: inglés]
[12 de mayo de 2022]

Capítulo 1. Disposiciones generales

Artículo. Disposiciones generales

La finalidad de la presente Convención es:

1. promover y fortalecer las medidas encaminadas a prevenir y combatir con mayor eficiencia y eficacia los delitos y otros actos ilícitos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas de tecnología de la información y las comunicaciones y los datos informáticos;
2. promover, facilitar y apoyar la cooperación internacional y la asistencia técnica a efectos de prevenir y combatir los delitos y otros actos ilícitos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas de tecnología de la información y las comunicaciones y los datos informáticos;
3. promover, facilitar y apoyar la cooperación internacional y la asistencia técnica en la recuperación de activos procedentes de los delitos y otros actos ilícitos mencionados en la presente Convención.

Artículo. Ámbito de aplicación

1. De conformidad con sus disposiciones, la presente Convención se aplicará a la prevención, la investigación y el enjuiciamiento de delitos, a la promoción, facilitación y apoyo de la cooperación internacional para prevenir y combatir la utilización de tecnologías de la información y las comunicaciones en la comisión de delitos y al embargo preventivo, la incautación, el decomiso y la restitución del producto de los delitos tipificados con arreglo a la presente Convención.
2. Para la aplicación de la presente Convención, a menos que contenga una disposición en contrario, no será necesario que los delitos tipificados en sus disposiciones produzcan daño o perjuicio a personas o bienes o al Estado.

Artículo. Protección de la soberanía

1. Los Estados parte cumplirán sus obligaciones con arreglo a la presente Convención en consonancia con los principios de soberanía, igualdad soberana e integridad territorial de los Estados, así como de no intervención en los asuntos internos de otros Estados parte o Estados que no son parte.
2. Nada de lo dispuesto en la presente Convención facultará a un Estado parte para ejercer, en el territorio de otro Estado parte o Estado que no sea parte, una jurisdicción o funciones que ese Estado parte o Estado que no sea parte reserve exclusivamente a sus autoridades conforme a su derecho interno y al derecho y las obligaciones internacionales.

Capítulo 2. Tipificación

Artículo. Acceso ilícito o no autorizado a sistemas o datos informáticos

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito el acceso deliberado e ilegítimo a todo o a parte de un sistema informático. Los Estados parte podrán exigir que el delito se cometa

incumpliendo o infringiendo una medida de seguridad o con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático (*Basado en el Convenio de Budapest, artículo 2 - Acceso ilícito*).

Artículo. Interceptación ilícita o no autorizada

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito, cuando se cometa intencionalmente, la interceptación ilegítima y sin autoridad de un sistema o datos informáticos en caso de que dicha interceptación tenga lugar por medios técnicos a fin de interceptar datos relativos al tráfico y datos procesados mediante tecnología de la información y las comunicaciones no destinados al uso público, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos.
2. Los Estados parte podrán exigir que el delito se cometa con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

Artículo. Ataques ilícitos a la integridad de los datos

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito todo acto deliberado e ilegítimo que introduzca, dañe, borre, deteriore, altere o suprima datos informáticos.
2. Los Estados parte podrán reservarse el derecho a exigir que los actos definidos en el párrafo 1 comporten daños graves.

Artículo. Ataques ilícitos a la integridad del sistema

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito la obstaculización deliberada, ilegítima y sin autoridad del funcionamiento de un sistema de tecnología de la información y las comunicaciones mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.
2. Cada Estado parte podrá reservarse el derecho a imponer un agravante de la pena en caso de que las acciones expuestas en el párrafo 1 tengan que ver con infraestructura crítica o afecten a esta.

Artículo. Uso indebido de dispositivos/programas maliciosos/programas informáticos

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito todo acto deliberado e ilegítimo destinado a:
 - a) la producción, venta, obtención para su utilización, importación, distribución u otra forma de puesta a disposición de:
 - i) cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos tipificados de conformidad con los artículos relativos al acceso no autorizado o ilícito, la interceptación no autorizada o ilícita o los ataques ilícitos a la integridad de los datos o del sistema;
 - ii) una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o a parte de un sistema de tecnología de la información y las comunicaciones, con intención de que sean utilizados para cometer cualquiera de los delitos tipificados de conformidad con los artículos relativos al acceso no autorizado o ilícito, la interceptación no autorizada o ilícita o los ataques ilícitos a la integridad de los datos o del sistema, y
 - b) la posesión de alguno de los elementos contemplados en los incisos a) i) o ii) del presente artículo con intención de que sean utilizados para cometer cualquiera de los delitos tipificados de conformidad con los artículos relativos al acceso no autorizado o ilícito, la interceptación no autorizada o ilícita o los ataques ilícitos a la integridad de

los datos o del sistema. Los Estados parte podrán exigir en su derecho interno la posesión de un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

2. No se interpretará que el presente artículo impone responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, distribución o cualquier otra forma de puesta a disposición mencionada en el párrafo 1 del presente artículo no tenga por objeto la comisión de uno de los delitos tipificados de conformidad con los artículos de la presente Convención relativos al acceso no autorizado o ilícito, la interceptación no autorizada o ilícita o los ataques ilícitos a la integridad de los datos o del sistema, como en el caso de las pruebas autorizadas o la protección de un sistema informático.

3. Los Estados parte podrán reservarse el derecho a no aplicar el párrafo 1 del presente artículo, siempre que dicha reserva no afecte a la venta, distribución o cualesquiera otras formas de puesta a disposición de los elementos mencionados en el artículo 1 a) ii) del presente artículo.

Artículo. Delitos relacionados con el contenido

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito toda conducta deliberada e ilegítima consistente en:

a) producir material que muestre explotación y abusos sexuales de niños mediante un sistema de tecnología de la información y las comunicaciones;

b) ofrecer o poner a disposición material que muestre explotación y abusos sexuales de niños mediante un sistema de tecnología de la información y las comunicaciones;

c) distribuir o transmitir material que muestre explotación y abusos sexuales de niños mediante un sistema de tecnología de la información y las comunicaciones;

d) adquirir para uno mismo o para otra persona material que muestre explotación y abusos sexuales de niños mediante un sistema informático o de tecnología de la información y las comunicaciones;

e) poseer material que muestre explotación y abusos sexuales de niños en un sistema informático o de tecnología de la información y las comunicaciones o en un dispositivo de almacenamiento de datos informáticos.

2. A los efectos del párrafo 1 anterior, se entenderá por “material que muestre explotación y abusos sexuales de niños” todo material que contenga la representación visual de:

a) un niño adoptando un comportamiento sexualmente explícito;

b) una persona con apariencia de niño adoptando un comportamiento sexualmente explícito;

c) imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito.

3. A los efectos del anterior párrafo 2, se entiende por “niño” todo ser humano menor de dieciocho (18) años de edad, salvo que, en virtud de la ley que le sea aplicable, haya alcanzado antes la mayoría de edad (Convención sobre los Derechos del Niño, artículo 1).

Artículo. Violación de la intimidad/Distribución no consentida de imágenes de contenido sexual

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito toda conducta deliberada e ilegítima consistente en:

a) publicar, distribuir, transmitir, vender, ofrecer o anunciar una imagen de carácter íntimo de alguien a sabiendas de que la persona representada en la imagen no ha dado su consentimiento al respecto;

b) publicar, distribuir, transmitir, vender, ofrecer o anunciar una imagen de carácter íntimo de alguien con intención de acosar o causar daño a la persona representada en la imagen;

Definición de “imagen de carácter íntimo”

2. A los efectos del presente artículo, se entiende por “imagen de carácter íntimo” un registro visual de una persona captado por cualquier medio, con inclusión de un registro fotográfico, filmico o videográfico:

a) en el que la persona aparece desnuda, expone sus genitales, su región anal o sus senos o realiza una actividad sexual explícita;

b) con respecto al cual en el momento del registro confluyeran circunstancias que dieran lugar a una expectativa razonable de privacidad, y

c) con respecto al cual la persona representada siga teniendo una expectativa razonable de privacidad en el momento en que se comete el delito.

Artículo. Propiedad intelectual

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito la violación de derechos de autor y otros derechos conexos definida en la legislación del Estado parte cuando esos actos se cometan intencionalmente mediante tecnología de la información y las comunicaciones y a escala comercial.

Delitos informáticos

Artículo. Falsificación informática

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente.

2. Los Estados partes podrán exigir que exista una intención dolosa o delictiva similar para que se considere que existe responsabilidad penal.

Artículo. Fraude informático

1. Cada Estado parte adoptará las medidas legislativas o de otra índole que resulten necesarias para tipificar como delito los actos deliberados y cometidos de forma ilegítima y sin autoridad que causen perjuicio patrimonial a otra persona mediante:

a) cualquier tipo de introducción, alteración, borrado o supresión de datos informáticos;

b) cualquier interferencia en el funcionamiento de un sistema informático;

con la intención, dolosa o delictiva, de obtener un beneficio económico para uno mismo o para otra persona.

Artículo. Actos delictivos preparatorios

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito cualquier forma de participación, ya sea como cómplice, colaborador, instigador, promotor o confabulador, en un delito tipificado con arreglo a la presente Convención.

2. Cada Estado parte podrá adoptar las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito cualquier tentativa de cometer un delito tipificado con arreglo a la presente Convención.
3. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito la preparación de un delito tipificado con arreglo a la presente Convención.

Artículo. Responsabilidad de las personas jurídicas

1. Cada Estado parte adoptará las medidas que resulten necesarias, de conformidad con sus principios jurídicos, a fin de establecer la responsabilidad de personas jurídicas por su participación en la comisión de un delito previsto en aplicación de la presente Convención, cuando este sea cometido por cuenta de las mismas por una persona física, ya sea a título individual o como miembro de un órgano de dicha persona jurídica, que ejerza funciones directivas en su seno, en virtud de:
 - a) un poder de representación de la persona jurídica;
 - b) una autorización para tomar decisiones en nombre de la persona jurídica;
 - c) una autorización para ejercer funciones de supervisión o control en el seno de la persona jurídica.
2. Además de los casos previstos en el párrafo 1 del presente artículo, cada Estado parte adoptará las medidas necesarias para garantizar que pueda exigirse responsabilidad a una persona jurídica cuando la ausencia de vigilancia o de control por parte de cualquier persona física mencionada en el párrafo 1 haya permitido la comisión de un delito previsto en aplicación del presente Convenio por una persona física que actúe por cuenta de dicha persona jurídica y bajo su autoridad expresa o tácita.
3. Con sujeción al derecho interno del Estado Parte, la responsabilidad de las personas jurídicas podrá ser de índole penal, civil o administrativa.
4. Dicha responsabilidad existirá sin perjuicio de la responsabilidad penal que incumba a las personas naturales que hayan cometido los delitos.
5. Cada Estado parte velará en particular por que se impongan sanciones penales o no penales eficaces, proporcionadas y disuasivas, incluidas sanciones monetarias, a las personas jurídicas consideradas responsables con arreglo al presente artículo.

Artículo. Sanciones y medidas

1. Cada Estado parte penalizará la comisión de un delito tipificado con arreglo a la presente Convención con sanciones acordes con la gravedad del delito y eficaces, proporcionadas y disuasivas, con inclusión de la privación de libertad.
2. Cada Estado parte garantizará la imposición de sanciones o medidas penales o no penales efectivas, proporcionadas y disuasorias, incluidas sanciones monetarias, a las personas jurídicas consideradas responsables de conformidad con el artículo relativo a la responsabilidad de las personas jurídicas.

Capítulo 3. Derecho procesal y aplicación de la ley

Artículo. Ámbito de aplicación de las disposiciones de procedimiento

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para establecer los poderes y procedimientos previstos en el presente capítulo a los efectos de investigaciones o procedimientos penales.
2. Salvo que se prevea lo contrario en el artículo relativo a la interceptación de comunicaciones, cada Estado parte aplicará los poderes y procedimientos mencionados en el párrafo 1 del presente artículo:
 - a) a los delitos tipificados de conformidad con los artículos de la presente Convención en materia de criminalización;

b) a cualquier otro delito cometido por medio de un sistema de tecnología de la información y las comunicaciones, y

c) a la obtención de pruebas electrónicas de cualquier delito.

3. Cada Estado parte podrá reservarse el derecho a aplicar las medidas mencionadas en el artículo relativo a la obtención de datos en tiempo real únicamente a los delitos o categorías de delitos especificados en su reserva, siempre que el repertorio de dichos delitos no sea más reducido que el de los delitos a los que dicho Estado parte aplique las medidas mencionadas en el artículo dedicado a la interceptación de datos relativos al contenido.

4. Cuando, a causa de las restricciones que imponga su legislación vigente en el momento de la adopción de la presente Convención, un Estado parte no pueda aplicar las medidas previstas en los artículos en materia de obtención de datos en tiempo real y de interceptación de datos relativos al contenido a las comunicaciones transmitidas dentro del sistema informático de un proveedor de servicios:

i) que se haya puesto en funcionamiento para un grupo restringido de usuarios, y

ii) que no emplee las redes públicas de telecomunicación y no esté conectado a otro sistema informático, ya sea público o privado,

dicho Estado parte podrá reservarse el derecho a no aplicar dichas medidas a esas comunicaciones.

5. Cada Estado parte tratará de limitar este tipo de reservas de modo que sea posible la más amplia aplicación de las medidas previstas en los artículos en materia de obtención de datos en tiempo real y de interceptación de datos relativos al contenido.

Artículo. Condiciones y salvaguardias

1. Cada Estado parte se asegurará de que la instauración, ejecución y aplicación de los poderes y procedimientos previstos en el presente artículo se sometan a las condiciones y salvaguardias previstas en su derecho interno, que deberá garantizar la protección de los derechos humanos y de las libertades fundamentales, en particular de los derechos derivados de las obligaciones que haya asumido cada Estado parte en virtud del Pacto Internacional de Derechos Civiles y Políticos de 1966 y otros instrumentos internacionales aplicables en materia de derechos humanos.

2. Cuando proceda, teniendo en cuenta la naturaleza del procedimiento o del poder de que se trate, dichas condiciones y salvaguardias incluirán una supervisión judicial u otra forma de supervisión independiente, los motivos que justifiquen su aplicación, así como la limitación del ámbito de aplicación y de la duración de dicho poder o procedimiento.

3. Siempre que sea conforme con el interés público, y en particular con la buena administración de la justicia, cada Estado parte examinará los efectos de los poderes y procedimientos mencionados en el presente artículo sobre los derechos, responsabilidades e intereses legítimos de terceros.

Artículo. Conservación rápida de datos informáticos

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para permitir a sus autoridades competentes ordenar o imponer de otro modo la obtención, acopio y conservación rápidas de datos electrónicos específicos, incluidos los datos relativos al tráfico, en particular cuando existan motivos para creer que dichos datos son particularmente susceptibles de eliminación, modificación o pérdida.

2. Cuando un Estado parte aplique lo dispuesto en el párrafo 1 anterior por medio de una orden impartida a una persona, incluso a una persona jurídica, a efectos de que conserve determinados datos informáticos almacenados que se encuentren en poder o bajo el control de esa persona, el Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para obligar a dicha persona a conservar y a preservar la integridad de esos datos durante el tiempo necesario, pero no superior al que

determine el derecho interno de dicho Estado parte, con el fin de que las autoridades competentes puedan obtener la revelación de los datos. Los Estados partes podrán prever la renovación de dicha orden.

3. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para obligar a la persona encargada de conservar la información a mantener en secreto la ejecución de dichos procedimientos durante el tiempo previsto en su derecho interno.

4. Los poderes y procedimientos mencionados en el presente artículo se establecerán conforme a lo dispuesto en los artículos relativos al ámbito de aplicación de las disposiciones de procedimiento y a las condiciones y salvaguardias.

Artículo. Conservación y revelación parcial rápidas de los datos relativos al tráfico

1. Con el fin de garantizar la conservación de los datos relativos al tráfico en aplicación del artículo relativo a la conservación rápida de los datos informáticos, cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para:

a) garantizar la conservación rápida de los datos relativos al tráfico, ya sean uno o varios los proveedores de servicios que participen en la transmisión de dicha comunicación, y

b) asegurar la revelación rápida a la autoridad competente del Estado parte, o a una persona designada por dicha autoridad, de un volumen suficiente de datos relativos al tráfico para que dicho Estado parte pueda identificar tanto a los proveedores de servicios como la vía por la que la comunicación se ha transmitido.

2. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos relativos al ámbito de aplicación de las disposiciones de procedimiento y a las condiciones y salvaguardias.

Artículo. Orden de presentación

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para facultar a sus autoridades competentes, cuando existan motivos razonables para creer que se ha cometido o se está cometiendo un delito, a ordenar:

a) a una persona, incluida una persona jurídica, presente en su territorio que comunique datos informáticos que obren en su poder o bajo su control, almacenados en un sistema informático o en un dispositivo de almacenamiento informático, y

b) a un proveedor que ofrezca sus servicios en el territorio de dicho Estado parte que comunique los datos que obren en su poder o bajo su control relativos a los abonados en relación con dichos servicios.

2. Los poderes y procedimientos mencionados en el presente artículo se establecerán conforme a lo dispuesto en los artículos relativos al ámbito de aplicación de las disposiciones de procedimiento y a las condiciones y salvaguardias.

3. A los efectos del presente artículo, se entenderá por “datos relativos a los abonados” cualquier información que posea un proveedor de servicios y que se refiera a los abonados de sus servicios, aparte de los datos relativos al tráfico o al contenido, y sirva para determinar:

a) el tipo de servicios de información y comunicaciones utilizado, las disposiciones técnicas adoptadas y el período de servicio;

b) la identidad, la dirección postal o situación geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso, con inclusión de direcciones IP y datos relativos a la facturación y al pago, disponibles en virtud de un contrato o de un acuerdo de prestación de servicio;

c) información relativa a la ubicación del equipo de información y telecomunicaciones que tenga repercusión en el contrato o acuerdo de prestación de servicio.

Artículo. Registro y confiscación de información almacenada o procesada electrónicamente

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para facultar a sus autoridades competentes, cuando existan motivos razonables para creer que se ha cometido o se está cometiendo un delito, a registrar o a tener acceso de un modo similar:

a) a todo sistema de tecnología de la información y las comunicaciones o a parte del mismo, así como a los datos informáticos en él almacenados, y

b) a todo dispositivo de almacenamiento informático que permita almacenar datos informáticos en su territorio.

2. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para asegurarse de que, cuando, de conformidad con el párrafo 1 a), sus autoridades registren o tengan acceso de un modo similar a un sistema informático específico o a una parte del mismo y tengan motivos razonables para creer que los datos buscados se hallan almacenados en otro sistema informático o en una parte del mismo situado en su territorio, y que dichos datos son legítimamente accesibles a partir del sistema inicial o están disponibles por medio de dicho sistema inicial, dichas autoridades puedan extender rápidamente el registro o el acceso de un modo similar al otro sistema.

3. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para facultar a sus autoridades competentes a confiscar o a obtener de un modo similar los datos informáticos a los que se haya accedido en aplicación de los párrafos 1 o 2. Estas medidas incluirán el poder para:

a) confiscar u obtener de un modo similar un sistema informático o una parte del mismo, o un dispositivo de almacenamiento de datos informáticos;

b) realizar y conservar una copia de esos datos informáticos;

c) preservar la integridad de los datos informáticos almacenados pertinentes;

d) hacer inaccesibles o suprimir dichos datos informáticos del sistema informático consultado.

4. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para facultar a sus autoridades competentes a ordenar a toda persona que conozca el funcionamiento de un sistema informático o las medidas aplicadas para proteger los datos informáticos que contiene, que proporcione toda la información necesaria, dentro de lo razonable, para permitir la aplicación de las medidas previstas en los párrafos 1, 2 y 3.

5. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos relativos al ámbito de aplicación de las disposiciones de procedimiento y a las condiciones y salvaguardias.

Artículo. Obtención en tiempo real de datos relativos al tráfico

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para facultar a sus autoridades competentes, cuando existan motivos razonables para creer que se ha cometido o se está cometiendo un delito:

a) a obtener o grabar con medios técnicos existentes en su territorio, y

b) a obligar a cualquier proveedor de servicios, en la medida de sus capacidades técnicas:

- i) a obtener o grabar con medios técnicos existentes en su territorio, o
 - ii) a prestar a las autoridades competentes su colaboración y su asistencia para obtener o grabar en tiempo real los datos relativos al tráfico asociados a comunicaciones específicas transmitidas en su territorio por medio de un sistema informático.
2. Cuando un Estado parte no pueda adoptar las medidas enunciadas en el párrafo 1 a) de conformidad con su derecho interno, podrá, en su lugar, adoptar las medidas legislativas y de otra índole que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos relativos al tráfico asociados a comunicaciones específicas transmitidas en su territorio mediante la aplicación de medios técnicos existentes en dicho territorio.
3. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se haya ejercido cualquiera de los poderes previstos en el presente artículo, así como toda información al respecto.
4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos relativos al ámbito de aplicación de las disposiciones de procedimiento y a las condiciones y salvaguardias.

Artículo. Interceptación de datos relativos al contenido

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias, en lo que respecta a un repertorio de delitos graves que deberá definirse en su derecho interno, para facultar a sus autoridades competentes, cuando existan motivos razonables para creer que se ha cometido o se está cometiendo un delito:
 - a) a obtener, grabar o almacenar con medios técnicos existentes en su territorio, y
 - b) a obligar a cualquier proveedor de servicios, en la medida de sus capacidades técnicas:
 - i) a obtener, grabar o almacenar con medios técnicos existentes en su territorio, o
 - ii) a prestar a las autoridades competentes su colaboración y su asistencia para obtener o grabar en tiempo real los datos relativos al contenido de comunicaciones específicas transmitidas en su territorio por medio de un sistema informático.
2. Cuando un Estado parte no pueda adoptar las medidas enunciadas en el párrafo 1 a) de conformidad con su derecho interno, podrá, en su lugar, adoptar las medidas legislativas y de otra índole que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos relativos al contenido de comunicaciones específicas transmitidas en su territorio mediante la aplicación de medios técnicos existentes en dicho territorio.
3. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se haya ejercido cualquiera de los poderes previstos en el presente artículo, así como toda información al respecto.
4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos relativos al ámbito de aplicación de las disposiciones de procedimiento y a las condiciones y salvaguardias.

Malasia

[Original: inglés]
[20 de abril de 2022]

Capítulo I. Disposiciones generales

Artículo 1. Finalidad

La finalidad de la presente Convención es:

- a) promover y fortalecer las medidas para prevenir y combatir o contrarrestar la ciberdelincuencia de forma más eficaz y eficiente;
- b) promover y facilitar la cooperación internacional;
- c) respaldar la creación de capacidad y la asistencia técnica para que los Estados Miembros puedan fortalecer su capacidad de hacer frente a la ciberdelincuencia, y
- d) garantizar el debido equilibrio entre los intereses de la aplicación de la ley y el respeto de los derechos humanos fundamentales.

Artículo 2. Definiciones

A los efectos de la presente Convención:

- a) se entenderá por “niño” toda persona menor de 18 años;
- b) se entenderá por “autoridad competente” toda autoridad judicial, administrativa o encargada de otra forma de la aplicación de la ley facultada por el derecho interno para ordenar, autorizar o llevar a cabo la ejecución de medidas previstas en la presente Convención en relación con investigaciones o procesos penales;
- c) “informático” hace referencia a un dispositivo electrónico, magnético, óptico, electroquímico o de procesamiento de datos por otros medios o a un grupo de dispositivos de ese tipo conectados entre sí o conexos que ejerza funciones lógicas, aritméticas, de almacenamiento y de visualización e incluya medios de almacenamiento de datos o de comunicaciones que guarden relación directa o funcionen junto con dicho dispositivo o grupo de dispositivos de ese tipo conectados entre sí o conexos, pero no incluirá una máquina de escribir o dispositivo de composición tipográfica automatizado ni una calculadora de mano portátil u otro dispositivo semejante que no sea programable o no contenga un medio de almacenamiento de datos;
- d) se entenderá por “delitos cibernéticos” los delitos tipificados de conformidad con la presente Convención;
- e) se entenderá por “datos” toda representación de información o de conceptos que se estén preparando o se hayan preparado en cualquier formato que se preste a tratamiento informático;
- f) la “función” consta de la lógica, el control, la aritmética, la eliminación, el almacenamiento y la recuperación y comunicación o telecomunicación dirigidos a un sistema informático, originados en un sistema informático o efectuados dentro del mismo;
- g) se entenderá por “programa” los datos que representen instrucciones o declaraciones que, ejecutadas en un sistema informático, hagan que este lleve a cabo una función.

Artículo 3. Ámbito de aplicación

1. A menos que contenga una disposición en contrario, la presente Convención se aplicará a la prevención, la investigación y el enjuiciamiento de los delitos tipificados en ella.
2. La Convención también podrá aplicarse, cuando así se indique, a la obtención de pruebas electrónicas de cualquier delito.

3. Se aplicará también a la oferta y prestación de asistencia técnica y creación de capacidad en asuntos abarcados por ella.

Artículo 4. Protección de la soberanía

1. Los Estados parte cumplirán sus obligaciones con arreglo a la presente Convención en consonancia con los principios de igualdad soberana e integridad territorial de los Estados, así como de no intervención en los asuntos internos de otros Estados.
2. Nada de lo dispuesto en la presente Convención facultará a un Estado parte para ejercer, en el territorio de otro Estado parte, una jurisdicción o funciones que ese Estado parte reserve exclusivamente a sus autoridades conforme a su derecho interno.

Capítulo II. Penalización y aplicación de la ley

Artículo 5. Acceso no autorizado

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito el acceso deliberado y no autorizado de cualquier tipo por una persona cualquiera a un programa del tipo que sea o datos almacenados en un sistema informático.

Artículo 6. Interceptación no autorizada

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito la interceptación deliberada y no autorizada de cualquier tipo por una persona cualquiera a datos o comunicaciones del tipo que sean.

Artículo 7. Ataques a la integridad de los datos

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado e ilegítimo que dañe, borre, deteriore o altere datos informáticos.
2. Los Estados parte podrán reservarse el derecho a exigir que los actos definidos en el párrafo 1 comporten daños graves.

Artículo 8. Obstrucción de un sistema informático, un programa o datos

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito la obstrucción grave deliberada de un programa o datos informáticos mediante su interferencia, interrupción, supresión, obstaculización del acceso o perjuicio.

Artículo 9. Uso indebido de datos, programas o sistemas informáticos

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito todo acto deliberado e ilegítimo destinado a la producción, adaptación, venta, obtención con fines de utilización, importación, oferta, distribución, suministro o cualquier otra forma de puesta a disposición de datos, programas o sistemas informáticos.

Artículo 10. Delitos relacionados con la pornografía infantil

1. Se tipificará como delito toda conducta deliberada e ilegítima consistente en:
 - a) elaborar o producir cualquier tipo de pornografía infantil o dirigir su elaboración o producción con la intención de difundirla a través de un sistema informático;
 - b) utilizar o hacer que se utilicen niños en los preparativos para elaborar o producir pornografía infantil o para dirigir esa elaboración o producción o en la elaboración o producción de pornografía infantil o en la dirección de esa elaboración o producción con fines de distribución mediante un sistema informático;

c) intercambiar, publicar, imprimir, reproducir, vender, poner en alquiler, distribuir, exhibir, anunciar, transmitir, promover, importar, exportar, trasladar, ofrecer o poner a disposición mediante un sistema informático cualquier tipo de pornografía infantil;

d) obtener, acopiar o buscar cualquier tipo de pornografía infantil a través de un sistema informático;

e) participar en los beneficios derivados de toda actividad comercial que, por lo que la persona sabe o tiene motivos para creer, guarda relación con cualquier tipo de pornografía infantil a través de un sistema informático o percibir dichos beneficios;

f) acceder a cualquier tipo de pornografía infantil a través de un sistema informático o tener ese material en poder o bajo control personal.

2. A efectos del párrafo 1, la expresión “pornografía infantil” aparece definida en el Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía.

Artículo 11. Tentativa y complicidad

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito, de conformidad con su derecho interno, cualquier forma de incitación o participación, ya sea como cómplice, colaborador o instigador, en un delito tipificado con arreglo a la presente Convención.

2. Cada Estado parte podrá adoptar las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito, de conformidad con su derecho interno, la preparación con miras a cometer un delito tipificado con arreglo a la presente Convención.

3. Cada Estado parte podrá adoptar las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito, de conformidad con su derecho interno, la preparación con miras a cometer un delito tipificado con arreglo a la presente Convención.

Artículo 12. Responsabilidad de las personas jurídicas

1. Cada Estado parte adoptará las medidas que resulten necesarias, en consonancia con sus principios jurídicos, a fin de establecer la responsabilidad de personas jurídicas por su participación en delitos tipificados con arreglo a la presente Convención.

2. Con sujeción a los principios jurídicos del Estado parte, la responsabilidad de las personas jurídicas podrá ser de índole penal, civil o administrativa.

3. Dicha responsabilidad existirá sin perjuicio de la responsabilidad penal que incumba a las personas naturales que hayan cometido los delitos.

4. Cada Estado parte velará en particular por que se impongan sanciones penales o no penales eficaces, proporcionadas y disuasivas, incluidas sanciones monetarias, a las personas jurídicas consideradas responsables con arreglo al presente artículo.

Artículo 13. Proceso, fallo y sanciones

1. Cada Estado parte penalizará la comisión de los delitos tipificados con arreglo a la presente Convención con sanciones que tengan en cuenta la gravedad de esos delitos.

2. Cada Estado parte velará por que se ejerzan cualesquiera facultades legales discrecionales de que disponga conforme a su derecho interno en relación con el enjuiciamiento de personas por los delitos comprendidos en la presente Convención a fin de dar máxima eficacia a las medidas adoptadas para hacer cumplir la ley respecto de esos delitos, teniendo debidamente en cuenta la necesidad de prevenir su comisión.

3. Cuando se trate de delitos tipificados con arreglo a la presente Convención, cada Estado parte adoptará medidas apropiadas, de conformidad con su derecho interno y tomando debidamente en consideración los derechos de la defensa, con miras a procurar

que, al imponer condiciones en relación con la decisión de conceder la libertad en espera de juicio o la apelación, se tenga presente la necesidad de garantizar la comparecencia del acusado en todo procedimiento penal ulterior.

4. Cada Estado parte velará por que sus tribunales u otras autoridades competentes tengan presente la naturaleza grave de los delitos comprendidos en la presente Convención al considerar la eventualidad de conceder la libertad anticipada o la libertad condicional a personas que hayan sido declaradas culpables de tales delitos.

5. Nada de lo dispuesto en la presente Convención afectará al principio de que la descripción de los delitos tipificados con arreglo a ella y de los medios jurídicos de defensa aplicables o demás principios jurídicos que regulan la legalidad de una conducta queda reservada al derecho interno de los Estados parte y de que esos delitos habrán de ser perseguidos y sancionados de conformidad con ese derecho.

Capítulo III. Procedimiento penal y aplicación de la ley

Artículo 14. Ámbito de aplicación de las medidas procesales

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para establecer los poderes y procedimientos previstos en el presente capítulo a los efectos de investigaciones o procedimientos penales.

2. Salvo que se establezca lo contrario, cada Parte aplicará los poderes y procedimientos mencionados en el párrafo 1 del presente artículo:

- a) a los delitos tipificados conforme a las definiciones de la presente Convención;
- b) a cualquier otro delito cometido por medio de un sistema informático, y
- c) a la obtención de pruebas electrónicas de cualquier delito.

Artículo 15. Orden de presentación

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para facultar a sus autoridades competentes a ordenar a una persona presente en su territorio que facilite datos informáticos específicos que obren en su poder o bajo su control, almacenados en un sistema informático o en un dispositivo de almacenamiento informático de datos.

Artículo 16. Registro y confiscación de datos informáticos almacenados

Cada Estado parte adoptará las medidas que resulten necesarias para facultar a sus autoridades competentes a registrar, confiscar y retener cualquier prueba de ese tipo, y las autoridades competentes tendrán derecho a acceder a todo tipo de programa o de datos presentes en cualquier sistema informático o tendrán derecho de acceso, inspección o verificación en relación con el funcionamiento de todo sistema informático o aparato o material conexo del que, sobre la base de motivos razonables, las autoridades competentes sospechen su utilización, actual o previa, en relación con cualquier delito previsto en la presente Convención.

Artículo 17. Jurisdicción

1. Cada Estado parte adoptará las medidas que resulten necesarias para establecer su jurisdicción respecto de los delitos tipificados con arreglo a la presente Convención cuando:

- a) el delito se cometa en su territorio, o
- b) el delito se cometa a bordo de un buque que enarbole su pabellón o de una aeronave registrada conforme a sus leyes en el momento de la comisión.

2. Con sujeción al artículo de la presente Convención relativo a la soberanía, un Estado Parte también podrá establecer su jurisdicción para conocer de tales delitos cuando:

- a) el delito se cometa contra uno de sus nacionales; o
- b) el delito sea cometido por uno de sus nacionales, o
- c) el delito se cometa contra el Estado Parte.

3. A los efectos del artículo de la presente Convención relativo a la extradición, cada Estado parte adoptará las medidas que resulten necesarias para establecer su jurisdicción respecto de los delitos tipificados con arreglo a la presente Convención cuando el presunto delincuente se encuentre en su territorio y el Estado parte no lo extradite por el solo hecho de ser uno de sus nacionales.

4. Cada Estado parte podrá también adoptar las medidas que resulten necesarias para establecer su jurisdicción respecto de delitos tipificados con arreglo a la presente Convención cuando el presunto delincuente se encuentre en su territorio y el Estado Parte no lo extradite.

5. Si un Estado parte que ejerce su jurisdicción con arreglo a los párrafos 1 o 2 del presente artículo ha recibido notificación, o tomado conocimiento por otro conducto, de que otros Estados parte están realizando una investigación, un proceso o una actuación judicial respecto de los mismos hechos, las autoridades competentes de esos Estados parte se consultarán, según proceda, a fin de coordinar sus medidas.

6. Sin perjuicio de las normas del derecho internacional general, la presente Convención no excluirá el ejercicio de las competencias penales establecidas por los Estados parte de conformidad con su derecho interno.

Artículo 18. Derechos de las víctimas

1. Cada Estado parte establecerá procedimientos adecuados que permitan a las víctimas de los delitos comprendidos en la presente Convención obtener indemnización.

2. Cada Estado parte permitirá, con sujeción a su derecho interno, que se presenten y examinen las opiniones y preocupaciones de las víctimas en las etapas apropiadas de las actuaciones penales contra los delincuentes sin que ello menoscabe los derechos de la defensa.

Singapur

[Original: inglés]
[28 de abril de 2022]

Disposiciones generales

Terminología y definiciones

2. Las definiciones terminológicas que se emplearán en la Convención deberán aclararse desde el principio. En particular, se han propuesto dos expresiones principales para describir el tema de la Convención: “ciberdelincuencia” y “utilización de las tecnologías de la información y las comunicaciones con fines delictivos”. El uso de “ciberdelincuencia” está ampliamente aceptado en relación con los delitos basados en la cibernética o facilitados por ella. La segunda expresión, “utilización de las tecnologías de la información y las comunicaciones con fines delictivos” abarcaría una amplia gama de asuntos relativos a la tecnología de las comunicaciones que exceden el ámbito de la “ciberdelincuencia”.

3. Singapur opina que la Convención debería basarse en el concepto de “ciberdelincuencia”, al tratarse de un término ampliamente aceptado que abarca las amenazas actuales y nuevas a las que se enfrentan los Estados Miembros en el ámbito de la ciberdelincuencia. De ese modo, la Convención se centrará con mayor precisión en los delitos que son específicos del ciberespacio o son posibles gracias a este y permitirá adoptar un enfoque más pragmático ante tales amenazas.

4. En la primera sesión también se deliberó sobre si en la Convención debería emplearse la expresión “prevenir y combatir” o “hacer frente”. Singapur prefiere que se emplee “prevenir y combatir”, que se ha empleado en instrumentos anteriores, como la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional.

Privacidad de los datos

5. Deberá encontrarse un equilibrio entre consideraciones relativas a la privacidad de los datos y la necesidad de garantizar la seguridad pública, en particular a efectos de luchar contra los delitos cibernéticos para garantizar la seguridad en línea y facultar a los organismos encargados de hacer cumplir la ley para que adopten las medidas necesarias de lucha rápida y efectiva contra la ciberdelincuencia.

Penalización y aplicación de la ley

6. La Convención debería comprender también las ciberestafas, que están basadas en la cibernética o se ven facilitadas por ella y actualmente constituyen un porcentaje desproporcionado del total de los casos de fraude a escala mundial. Solo en Singapur, las víctimas de estafas perdieron por lo menos 633,3 millones de dólares singapurenses en 2021, y se registró un aumento del 52,9 % en el número de casos de estafa con respecto al año anterior, lo cual supuso más de la mitad del total de delitos. Las agrupaciones de estafadores cuentan con abundantes recursos y hacen uso de la tecnología para estafar a través de las fronteras nacionales borrando las huellas.

7. A continuación se presenta texto sugerido por Singapur. Creemos que estas sugerencias constituyen un punto de partida realista y razonable para conseguir que las principales ciberestafas queden comprendidas en la Convención.

Acceso ilícito

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito el acceso deliberado e ilegítimo a todo o a parte de un sistema informático.

2. Los Estados parte podrán exigir que el delito se cometa infringiendo una medida de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, como asumir la identidad de otra persona, o en relación con un sistema informático conectado a otro sistema informático.

Ciberestafas

Cada Estado parte adoptará las medidas legislativas o de otra índole que resulten necesarias para tipificar como delito los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona o una entidad mediante:

- a) cualquier tipo de introducción, alteración, eliminación o supresión de datos informáticos;
- b) cualquier interferencia en el funcionamiento de un sistema informático;
- c) el uso de un sistema informático para engañar o inducir a otra persona o a una entidad para que haga o deje de hacer algo que la persona o entidad no haría o dejaría de hacer de otro modo, con la intención, dolosa o delictiva, de obtener de forma ilegítima para uno mismo o para otra persona:
 - i) un beneficio económico, y/o
 - ii) datos informáticos o información personal que el autor no tendría a su disposición de otro modo.

Acceso ilícito a contraseñas y credenciales

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado

e ilegítimo de adquisición, obtención, recepción o distribución de contraseñas o credenciales de acceso a un sistema informático o a datos informáticos.

Medidas procesales y aplicación de la ley

Conservación, acopio, obtención e intercambio de pruebas y datos electrónicos

8. Con respecto a la conservación, acopio, obtención e intercambio de pruebas y datos electrónicos, deseamos formular tres consideraciones:

a) Ahora que se almacenan en nube más datos y se llevan a cabo más transacciones digitales, las investigaciones penales, sobre todo las correspondientes a la ciberdelincuencia, comportan principalmente pruebas digitales. Las investigaciones y los enjuiciamientos se verán menoscabados si no se conservan, acopian y obtienen pruebas digitales de forma oportuna.

b) Las solicitudes de pruebas digitales por conducto de los canales existentes, como tratados de asistencia judicial recíproca, comportan procesos prolongados. Si no se conservan, acopian y obtienen pruebas digitales de forma oportuna, es muy probable que esas pruebas ya se hayan borrado cuando los países decidan acceder a la solicitud en el marco de uno de estos tratados. Así pues, recalcamos la necesidad de medidas para presentar legalmente solicitudes de conservación rápida de datos.

c) La ciberdelincuencia tiene carácter transnacional. Los avances tecnológicos han permitido a los delincuentes llevar a cabo sus actividades a distancia y a través de las fronteras nacionales. Las disposiciones encaminadas al intercambio transfronterizo de pruebas y datos electrónicos permitirán a nuestros organismos encargados de hacer cumplir la ley recabar pistas prácticas para llevar a cabo sus investigaciones y facilitarán la aprehensión efectiva y el ulterior enjuiciamiento de los delincuentes y la recuperación de activos. La Convención debería ofrecer a las Partes la opción de rechazar una solicitud si acceder a ella podría atentar contra la soberanía, la seguridad, el orden público u otros intereses esenciales de la Parte requerida.

9. Asimismo, señalamos que los Estados Miembros presentan ordenamientos jurídicos y circunstancias que, en última instancia, podrían afectar a su capacidad de aplicar medidas procesales, en particular con respecto a la obtención e interceptación de datos en tiempo real. Observamos que, en la mayoría de los casos de ciberdelincuencia, la inclusión de medidas de conservación, acopio, obtención e intercambio de pruebas y datos electrónicos ya favorecería considerablemente los procesos de investigación, especialmente en un tratado multilateral que cuente con un amplio apoyo de los Estados. Así pues, debemos evitar un exceso de prescripciones en relación con los procesos operacionales para que las disposiciones de la Convención sean aplicables a la mayoría de los Estados, lo cual ampliaría el grado de adhesión o ratificación. A su vez, ello nos permitiría abordar la ciberdelincuencia más efectivamente de forma concertada a escala mundial.

Recuperación de activos

10. Singapur ha oído a muchos Estados Miembros proclamar la necesidad de un mecanismo de recuperación de activos. Coincidimos en ello. Los grupos de ciberdelincuencia organizan operaciones transnacionales sofisticadas que no son fáciles de detectar o desmantelar. Cuentan con abundantes recursos y son adeptos de la utilización de tecnología para borrar las propias huellas. Cuando el producto del delito ya se ha retirado de un país, la recuperación resulta a menudo muy difícil.

11. En consecuencia, la presente Convención ofrece la oportunidad de aplicar medidas mundiales concretas, oportunas, eficientes y concertadas para recuperar activos, en vista de que la capacidad de cualquier país de recuperar el producto del delito que ya se ha retirado de su jurisdicción dependerá de la cooperación de organismos del extranjero encargados de hacer cumplir la ley. Es importante que los países colaboren en la recuperación de activos para que las organizaciones delictivas no perciban el producto del delito ni ganen en capacidad, competencia y sofisticación.

Uruguay

[Original: inglés]
[6 de mayo de 2022]

1. La presente Convención tendrá en cuenta los instrumentos internacionales y las iniciativas existentes en los planos nacional, regional e internacional para prevenir y combatir la utilización de las tecnologías de la información y las comunicaciones con fines delictivos en consonancia con la resolución 74/247 de la Asamblea General.

En ese sentido, la Convención también debería incorporar una disposición sobre la relación entre la Convención y otros instrumentos anteriores, en particular respecto de asuntos como la aplicación prioritaria y la no exclusión.

El Uruguay considera que en el texto debería figurar como disposición general un llamamiento a la coherencia dentro del sistema de las Naciones Unidas en cuanto a la prevención de la utilización ilícita de las tecnologías de la información y las comunicaciones y la correspondiente lucha.

2. La Convención debería disponer de un mecanismo flexible de seguimiento y revisión que tenga en cuenta los progresos y los cambios permanentes existentes en ese sentido.

También debería basarse en formulaciones tecnológicas neutrales y evitar la utilización de formulaciones vinculadas con un determinado sistema operativo o programa informático, con el objeto de ofrecer un enfoque más amplio que pueda interpretarse en el contexto de un entorno en rápida evolución.

El Uruguay considera importante que la Convención permita formular declaraciones interpretativas, además de incorporar un procedimiento de enmienda ágil para facilitar su actualización, y que establezca mecanismos para dirimir controversias.

Debería celebrarse periódicamente una conferencia de las partes para estudiar los cambios significativos en este ámbito y reflejarlos en el contenido de la Convención. El párrafo 1 del artículo 69 de la Convención de las Naciones Unidas contra la Corrupción sirve de guía:

La Conferencia de los Estados Parte hará todo lo posible por lograr un consenso sobre cada enmienda. Si se han agotado todas las posibilidades de lograr un consenso y no se ha llegado a un acuerdo, la aprobación de la enmienda exigirá, en última instancia, una mayoría de dos tercios de los Estados Parte presentes y votantes en la reunión de la Conferencia de los Estados Parte.

3. Deberán tenerse en cuenta las oportunidades de que el sector privado, la sociedad civil y el mundo académico participen y presenten aportaciones.

4. Por lo que se refiere a la jurisdicción internacional, el Uruguay considera que la cuestión del solapamiento de las jurisdicciones de dos o más Estados debería abordarse teniendo en cuenta la prioridad temporal en la investigación y la fecha de la reclamación.

No obstante, si un Estado parte que ejerce su jurisdicción respecto de un delito tipificado con arreglo la Convención que se haya cometido en su territorio a bordo de un buque que enarbole su pabellón; o a bordo de una aeronave registrada conforme a la legislación de esa Parte ha recibido notificación, o tomado conocimiento por otro conducto, de que otros Estados parte están realizando una investigación, un proceso o una actuación judicial respecto del mismo hecho, las autoridades competentes de esos Estados parte se consultarán, según proceda, a fin de coordinar sus medidas.

La Parte también adoptará las medidas previstas en la presente Convención cuando el delincuente se halle en el territorio de su país y no pueda ser extraditado a causa de su nacionalidad. El Estado en cuyo territorio se encuentre el autor de los delitos previstos en la presente Convención presentará el caso sin mayor dilación a sus autoridades competentes con fines de enjuiciamiento de conformidad con el derecho de ese Estado.

5. La lucha contra la ciberdelincuencia es un desafío oportuno y acuciante que deberá abordarse teniendo en cuenta la protección, el respeto y la efectividad de los derechos humanos y libertades fundamentales.

Todo lo que se dispone en la presente Convención se interpretará y utilizará conforme a las correspondientes obligaciones internacionales en el ámbito de los derechos humanos. En consecuencia, en el preámbulo deberá figurar un párrafo en el que se reafirmen la Declaración Universal de Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos y otros instrumentos pertinentes de derechos humanos.
