Naciones Unidas A/AC.291/9/Add.1

Asamblea General

Distr. general
21 de abril de 2022
Español
Original: árabe/español/francés/
inglés/ruso

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 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

V.22-02332 (S) 250522 250522

Índice

III. Disposiciones generales

Angola

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

Disposiciones generales

Definiciones: ciberdelincuencia, pruebas electrónicas, interceptación, sistema informático, datos informáticos, metadatos, datos de tráfico, proveedores de servicios, programa informático, red de comunicaciones electrónicas, infraestructura crítica, topografía, producto semiconductor, soberanía del ciberespacio.

Para elaborar definiciones de los conceptos aquí sugeridos se puede recurrir a los instrumentos jurídicos regionales e internacionales mencionados anteriormente[1].

Australia

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

Las disposiciones generales deberían incluir:

- una declaración de la finalidad claramente centrada en la lucha contra la ciberdelincuencia;
- el ámbito de aplicación, con metas concretas y claramente definido;
- definiciones consensuadas, que solo deberían examinarse y acordarse una vez resueltos los artículos sustantivos de la convención.

La naturaleza del ciberespacio, por cuanto se diferencia del espacio físico, añade complejidad a la implementación e interpretación de las normas y principios del derecho internacional, incluido el principio de soberanía de los Estados, y a la aplicación de la competencia territorial. Australia sugiere que las deliberaciones sobre la forma de tratar estas cuestiones jurídicas en la convención continúen en paralelo a la elaboración de las disposiciones sustantivas.

Brasil

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

Capítulo I
Disposiciones generales

Artículo 1
Propósito[2]

El propósito de esta Convención es prevenir y combatir la ciberdelincuencia estableciendo:

a) conductas que las partes han de castigar como delitos en sus territorios;

[1] Nota de la Secretaría: se refiere a los instrumentos incluidos en un apartado diferente: Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales, Convenio sobre la Ciberdelincuencia del Consejo de Europa, Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y Convención de las Naciones Unidas contra la Corrupción.

[2] *Fuente*: propuesta original presentada por el Brasil.

b) facultades procesales para la actuación oportuna de las autoridades nacionales, y

c) medidas de cooperación internacional.

Artículo 2
Ámbito de aplicación[3]

1. Esta Convención se aplicará a lo siguiente:

a) la prevención, la detección, la disrupción, la investigación, el enjuiciamiento y la resolución de los delitos cibernéticos;

b) la aplicación de medidas para mitigar las consecuencias de los delitos cibernéticos, y

c) toda forma pertinente de cooperación internacional para prevenir y combatir los delitos cibernéticos.

2. A los efectos de la aplicación de esta Convención, no será necesario que los delitos ocasionen daños materiales, salvo que se disponga lo contrario en ella.

Artículo 3
Definiciones[4]

A los efectos de la presente Convención:

a) Por “persona afectada” se entenderá toda persona, proveedor de servicios u otra entidad que se haya visto, o probablemente se vea, afectada por la concesión de cualquier orden en esta parte;

b) “Datos informáticos” incluirá toda representación de datos o información que haya sido, o pueda ser, almacenada, transmitida o procesada de otro modo en un sistema informático. Incluye datos de los abonados, de tráfico y de contenidos;

c) Por “sistema informático” se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el almacenamiento, la transmisión o el procesamiento de datos informáticos en ejecución de un programa u otro *software*;

d) Por “datos de contenido” se entenderá todo dato informático almacenado por un proveedor de servicios o cualquier otra información distinta de los datos de tráfico o de los abonados, como texto, voz, videos, imágenes y sonido, o el contenido de una comunicación;

e) Por “red de comunicaciones electrónicas” se entenderá los sistemas de transmisión, basados o no en una infraestructura permanente o en una capacidad de administración centralizada, y, en su caso, los equipos de conmutación o enrutamiento y otros recursos, incluidos los elementos de red que no son activos, que permiten el transporte de señales por cable, radio, medios ópticos u otros medios electromagnéticos, incluidas las redes de satélites, las redes fijas y móviles y los sistemas de cableado eléctrico, en la medida en que se utilicen para la transmisión de señales, con independencia del tipo de información transmitida;

f) Por “pruebas electrónicas” se entenderá todo dato o información generada, almacenada, transmitida o procesada de otro modo en forma electrónica que pueda utilizarse para probar o refutar un hecho en un procedimiento judicial;

g) Por “vigilancia electrónica” se entenderá:

[3] Propuesta presentada por China y Rusia, con cambios incorporados por el Brasil.

[4] Reunión del grupo de expertos para actualizar la Ley Modelo de Asistencia Judicial Recíproca en Asuntos Penales de la Oficina de las Naciones Unidas contra la Droga y el Delito (proceso en curso al 9 de marzo de 2022), con pequeños cambios incorporados por el Brasil.

i) el seguimiento, la interceptación, la copia o la manipulación de mensajes, datos o señales que hayan sido almacenados o transmitidos, o estén en proceso de transmisión, por medios electrónicos, o

ii) la vigilancia o grabación de actividades por medios electrónicos;

h) Por “proveedor de servicios” se entenderá:

i) cualquier persona, o entidad pública o privada, que proporcione a los usuarios de su servicio la posibilidad de comunicarse mediante un sistema informático, o que facilite de otro modo la comunicación a través de una red de comunicaciones electrónicas, o

ii) cualquier otra persona, o entidad pública o privada, que almacene o procese de otro modo datos informáticos en nombre de dicho servicio o de los usuarios de dicho servicio;

i) Por “datos del abonado” se entenderá todo dato informático, recogido en el curso normal de la actividad de un proveedor de servicios, relativo al nombre, la fecha de nacimiento, la dirección postal o geográfica, los datos de facturación y de pago, los identificadores del dispositivo, el número de teléfono o la dirección de correo electrónico, o cualquier otra información, como la dirección IP utilizada en el momento de la creación de una cuenta, que pueda servir para identificar al abonado o al cliente, así como el tipo de servicio prestado y la duración del contrato con el proveedor de servicios, que no sean datos de tráfico o de contenido;

j) Por “datos de tráfico” se entenderá todo dato informático recogido en el curso normal de la actividad de un proveedor de servicios, relacionado con:

i) el tipo de servicio prestado y su duración, cuando se trate de datos técnicos y de datos que identifiquen las medidas técnicas o las interfaces conexas utilizadas por el abonado o el cliente o que se le hayan proporcionado, así como los datos relativos a la validación del uso del servicio, con exclusión de las contraseñas u otros medios de autenticación utilizados en lugar de una contraseña que sean facilitados por un usuario, o creados a petición de un usuario; o

ii) el inicio o fin de la sesión de un usuario en un servicio, como la fecha y hora en que se utilizó, o el acceso al servicio y el cierre de sesión, o

iii) los metadatos de las comunicaciones, como se procesan en una red de comunicaciones electrónicas con el fin de transmitir, distribuir o intercambiar contenidos de comunicaciones electrónicas, incluidos los datos utilizados para rastrear y determinar el origen y el destino de una comunicación, los datos sobre la ubicación del equipo terminal procesados en el contexto de la prestación de servicios de comunicaciones, y la fecha, la hora, la duración y el tipo de comunicación.

Burundi

[Original: francés]
[8 de abril de 2022]

Capítulo I. Definiciones

A los efectos de la presente Convención:

a) Por “acceso ilícito” se entenderá el acceso intencional, sin que se tenga derecho a ello, a la totalidad o una parte de una red de comunicaciones electrónicas, de un sistema informático o de un equipo terminal;

b) Por “cifrado” se entenderá toda técnica que consista en transformar datos digitales en un formato ininteligible mediante el empleo de medios de criptología;

c) Por “criptología” se entenderá la ciencia relativa a la protección y seguridad de la información;

d) Por “ciberdelincuencia” se entenderá todo hecho ilegal cometido mediante un sistema o red informática u otra red física conexa o en relación con un sistema informático;

e) Por “ciberespacio” se entenderá un conjunto de datos numéricos que constituyen un universo de información y un entorno de comunicación relacionado con la interconexión mundial de equipo para el procesamiento automatizado de datos numéricos;

f) Por “ciberseguridad” se entenderá un conjunto de medidas de prevención, protección y disuasión de tipo técnico, organizacional, jurídico, financiero, humano y procedimental y otras medidas que permiten alcanzar esos objetivos;

g) Por “comunicación electrónica” se entenderá toda emisión, transmisión o recepción de señas, señales, texto, imágenes, audio o video por medios electromagnéticos, ópticos o de otro tipo;

h) Por “datos personales” se entenderá toda información del carácter que sea e independientemente del soporte, incluidos audio e imágenes, relativa a una persona física identificada o identificable directa o indirectamente, en referencia a un número de identificación o a uno o varios elementos específicos propios de su identidad física, fisiológica, genética, psíquica, cultural, social o económica;

i) Por “datos informáticos” se entenderá toda representación de hechos, información o conceptos de una forma que se preste al procesamiento en un sistema informático, incluido un programa del tipo que pueda asegurar que un sistema informático ejecute una función;

j) Por “electromagnético” se entenderá el resultado de la vibración combinada de un campo eléctrico y un campo magnético variable en el tiempo;

k) Por “proveedor de servicios” se entenderá una persona física o jurídica que presta uno o varios servicios a los usuarios de un sistema de telecomunicaciones;

l) Por “información” se entenderá todo elemento de conocimiento que puede ser representado mediante convenciones para su utilización, conservación, procesamiento o comunicación. La información puede expresarse en forma escrita, visual, sonora, digital o de otro tipo;

m) Por “infraestructura crítica” se entenderá la infraestructura que es esencial para los servicios vitales para la seguridad pública, la estabilidad económica, la seguridad nacional, la estabilidad internacional y la sostenibilidad y el restablecimiento del ciberespacio fundamental. La infraestructura crítica del Estado está constituida por los servicios de salud pública, seguridad interior y exterior, defensa, finanzas y transporte, que están conectados a redes de Internet;

n) Por “interceptación ilegal” se entenderá el acceso sin que medie derecho o autorización a datos de una red de comunicaciones electrónicas, de un sistema informático o de un equipo terminal;

o) “Pasarela internacional” es el nombre genérico de un dispositivo que permite comunicar dos redes informáticas de tipos diferentes, por ejemplo, una red local e Internet;

p) Por “medio de pago electrónico” se entenderá un medio que permite a su titular efectuar operaciones electrónicas de pago en línea;

q) Por “*phishing”* se entenderá una forma de engaño por correo electrónico que consiste en adoptar la identidad de una empresa conocida y reconocida en un mensaje de correo electrónico para incitar a los destinatarios a cambiar o actualizar sus datos bancarios en páginas de Internet que imitan las de la empresa cuya imagen se ha utilizado para el engaño;

r) Por “pornografía infantil” se entenderá toda representación visual de un componente sexualmente explícito, incluidas fotografías, películas, videos, imágenes creadas o producidas por vía electrónica, mecánica o de otro tipo, en que:

i) la producción de esta representación visual implique a un menor de edad;

ii) la representación visual sea una imagen digital, de computadora o generada por computadora en que haya un menor que participe en una conducta sexualmente explícita o en que se creen o utilicen imágenes de los órganos sexuales de un menor para fines principalmente sexuales y se exploten con o sin conocimiento del niño;

iii) la representación visual haya sido creada, adaptada o modificada para que parezca que hay un menor que participa en una conducta sexualmente explícita;

s) Por "prestador de servicios" se entenderá un operador de servicios móviles, de acceso a Internet y de infraestructura;

t) Por "programa informático" se entenderá un conjunto de instrucciones ejecutadas por la computadora para obtener los resultados esperados;

u) Por "racista y xenófobo en el entorno de las tecnologías de la información y las comunicaciones" se entenderá todo material escrito, imagen u otra representación de ideas o teorías que aliente o promueva el odio, la discriminación o la violencia contra una persona o grupo de personas por motivos de raza, color, ascendencia u origen nacional o étnico o religión;

v) Por "envío de correo basura" se entenderá el envío generalmente masivo y sin un destinatario concreto de mensajes comerciales por correo electrónico con el objetivo de cometer un robo contra personas que no han dado su autorización al emisor para recibir tales mensajes;

w) Por "sistema informático" se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí que realiza o en que diversos elementos realizan, al ejecutar un programa, el procesamiento automatizado de datos;

x) Por "TIC" se entenderá "tecnologías de la información y las comunicaciones".

Canadá[5]

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

Disposiciones generales

Finalidad

La finalidad de la presente Convención es promover la cooperación para prevenir, investigar y enjuiciar más eficazmente la ciberdelincuencia.

Ámbito de aplicación

Esta Convención se aplicará, salvo que se disponga lo contrario y con sujeción a las salvaguardas del caso, para:

a) promover y facilitar medidas legislativas y de otro tipo dirigidas a prevenir, investigar y enjuiciar la ciberdelincuencia y los delitos graves que se cometen frecuentemente utilizando sistemas informáticos, de conformidad con lo dispuesto en ella;

b) promover, facilitar y apoyar la asistencia y la cooperación en el ámbito internacional en relación con la prevención, investigación y enjuiciamiento de los delitos establecidos en ella;

[5] Nota de la Secretaría: el Canadá también presentó una lista de definiciones, que puede consultarse en www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-second-session.html.

c) promover, facilitar y apoyar una asistencia judicial recíproca eficiente y eficaz en relación con las pruebas electrónicas vinculadas a los delitos establecidos en ella y otras infracciones penales, y

d) promover, facilitar y apoyar la asistencia técnica en la prevención y la lucha contra la ciberdelincuencia.

Condiciones y salvaguardias

1. Cada Estado parte se asegurará de que la instauración, ejecución y aplicación de las disposiciones de esta Convención se sometan a las condiciones y salvaguardias previstas en su derecho interno, que deberá garantizar una protección plena de los derechos humanos y de las libertades, y en particular de los derechos derivados de las obligaciones que haya asumido en virtud del Pacto Internacional de Derechos Civiles y Políticos u otros instrumentos internacionales aplicables en materia de derechos humanos, y que deberá integrar los principios del estado de derecho, la legalidad, la necesidad y la proporcionalidad.

2. Cuando proceda, teniendo en cuenta la naturaleza del procedimiento o de la facultad 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 dicha facultad o procedimiento.

3. Cada Estado parte ha de aplicar medidas para mejorar la comprensión de los vínculos entre las cuestiones de género y la ciberdelincuencia, incluidas las formas en que esta puede afectar a las mujeres y los hombres de manera diferente. Las medidas han de tener por objetivo promover la igualdad de género y el empoderamiento de las mujeres, entre otras cosas, incorporando estas cuestiones en la legislación pertinente, la elaboración de políticas, la investigación, los proyectos y los programas, según proceda y de conformidad con los principios fundamentales del derecho interno.

4. Las medidas contenidas en esta Convención han de interpretarse y aplicarse de manera que no interfiera con la libertad de expresión, incluida la libertad de recabar, recibir y difundir información e ideas de toda índole, sin limitaciones de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro medio que se elija, y los derechos aplicables vinculados al respeto de la privacidad y la protección de datos. La interpretación y aplicación de esas medidas estarán en consonancia con los principios de no discriminación internacionalmente reconocidos.

Participación y tentativa

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito, de conformidad con su derecho interno, cualquier forma de 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 sean necesarias para tipificar como delito, de conformidad con su derecho interno, toda tentativa de cometer un delito tipificado con arreglo a la presente Convención.

3. Cada Estado parte podrá adoptar las medidas legislativas y de otra índole que sean 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.

Responsabilidad de las empresas

1. Cada Estado parte adoptará las medidas legislativas y de otro tipo que sean necesarias, en consonancia con sus principios jurídicos, a fin de establecer la responsabilidad de personas jurídicas por su participación en la comisión de los delitos tipificados con arreglo a la 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 perpetrado 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.

Colombia

[Original: español]
[9 de abril de 2022]

Disposiciones generales

Los Estados partes deben, al prevenir y combatir el delito cibernético en todos sus aspectos, promover y garantizar el pleno respeto de los derechos de las mujeres y las niñas y a su vez prestar especial atención a las cuestiones género, en particular a la violencia de género, incluida la violencia contra las mujeres y las niñas.

Los Estados partes deben, al prevenir y combatir el delito cibernético en todas sus expresiones, promover y garantizar el respeto de los derechos humanos y las libertades fundamentales. Todas las disposiciones de esta convención o instrumento se entenderán y aplicarán de manera concordante con las respectivas obligaciones internacionales en materia de derechos humanos.

Definiciones

Conforme al consenso establecido en la primera ronda de negociación respecto a la necesidad de acordar terminología y definiciones tecnológicamente neutras, aunado a lo expresado por el equipo del Consejo de Europa para el Convenio de Budapest, las definiciones contempladas tanto en el Convenio de Budapest como en su Segundo Protocolo resultan pertinentes, suficientes y adaptables a la evolución tecnológica, para ser propuestas ante el Comité Especial.

Así, las definiciones a proponer son:

a) Sistema informático: “todo dispositivo aislado o conjunto de dispositivos interconectados […] cuya función […] sea el tratamiento automatizado de datos en ejecución de un programa”;

b) Datos informáticos: “toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función”;

c) Proveedor de servicios: “toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático, y cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo”;

d) Datos relativos al tráfico: “todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente”;

e) Autoridad central: “la autoridad o autoridades designadas en virtud de un tratado o acuerdo de asistencia mutua basado en la legislación uniforme o recíproca en vigor entre las partes de que se trate, o en su defecto, la autoridad o autoridades designadas por una parte […] encargadas de enviar las solicitudes de asistencia mutua

o de responder a las mismas, de ejecutarlas o de remitirlas a las autoridades competentes para su ejecución";

f) Autoridad competente: "una autoridad judicial y administrativa o policial facultada por el derecho interno, para ordenar, autorizar o llevar a cabo la ejecución de medidas […] a efectos de la obtención o la presentación de pruebas en relación con investigaciones o procesos penales específicos";

g) Emergencia: "situación en la que existe un riesgo significativo e inminente para la vida o la seguridad de una o más personas físicas";

h) Datos personales: "la información relativa a una persona física identificada o identificable";

i) Parte transmitente: "la parte que transmite los datos en respuesta a una solicitud o en un equipo conjunto de investigación, o […] la parte en cuyo territorio se encuentre un proveedor de servicios transmitente o una entidad que preste servicios de registro de nombres de dominio";

j) Datos relativos a los abonados: "cualquier información […] que posea un proveedor de servicios y que se refiera a los abonados de sus servicios, diferentes de los datos relativos al tráfico o al contenido, y que permitan determinar […] el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio […] la identidad, la dirección postal o situación geográfica y el número de teléfono del abonado […] los datos relativos a la facturación y al pago […] cualquier otra información relativa al lugar en que se encuentren los equipos de comunicación".

Egipto

[Original: árabe]
[8 de abril de 2022]

Capítulo I. Disposiciones generales

Se propone que este capítulo abarque los objetivos de la convención, los términos utilizados, la protección de la soberanía y el ámbito de aplicación, como sigue:

Artículo 1. Objetivos

La presente Convención tiene por objeto reforzar la cooperación entre los Estados Miembros de las Naciones Unidas para luchar contra el uso de las tecnologías de la información y las comunicaciones con fines delictivos. Pretende suprimir las acciones que amenacen la integridad y la confidencialidad de las tecnologías de la información y las comunicaciones, tipificar como delito el uso indebido de estas tecnologías con fines ilícitos, facilitar la investigación y el enjuiciamiento de los autores y aplicar medidas para eliminar las consecuencias de tales delitos. Estas medidas incluyen la suspensión de las transacciones relacionadas con los activos obtenidos de la comisión de cualquier acto ilegal establecido en la Convención y el decomiso y la restitución del producto del delito. Para ello, la Convención prevé competencias suficientes para combatir eficazmente los delitos relacionados con las tecnologías de la información y las comunicaciones mediante el establecimiento de acuerdos de cooperación internacional encaminados a facilitar la detección e investigación de estos delitos, el enjuiciamiento de los autores y la extradición de los delincuentes.

Artículo 2. Términos empleados

Los siguientes términos, empleados en la presente Convención, tendrán el significado que se indica a continuación:

a) Tecnología de la información: cualquier medio físico o no corpóreo, o grupo de medios interconectados o no, utilizado para almacenar, ordenar, organizar, recuperar, procesar, desarrollar e intercambiar información según las órdenes e instrucciones

almacenadas en él, incluyendo todas las entradas y salidas asociadas a este medio, por cable o de forma inalámbrica, en un sistema o red;

b) Proveedor de servicios: toda persona física o jurídica, pública o privada, que proporciona a los abonados servicios para comunicarse a través de las tecnologías de la información o que procesa o almacena información en nombre de un servicio de comunicación o de sus usuarios;

c) Datos: toda información que pueda ser almacenada, procesada, generada y transmitida por la tecnología de la información, como números, letras, símbolos, etc.

d) Sistema de información: conjunto de programas e instrumentos diseñados para procesar y gestionar datos e información;

e) Red de información: dos o más sistemas de información que están conectados para obtener e intercambiar información;

f) Sitio: lugar donde se pone a disposición la información en una red de información a través de una dirección específica;

g) Captura: la visualización u obtención de datos o información;

h) Administrador del sitio: cualquier persona que sea responsable de organizar, gestionar, supervisar o mantener uno o más sitios en una red de información, incluidos los derechos de acceso para los diferentes usuarios en el sitio, de diseñar el sitio, de generar y organizar las páginas o contenidos del sitio, o del propio sitio;

i) Cuenta privada: conjunto de información relativa a una persona física o jurídica que le otorga el derecho exclusivo a acceder o utilizar los servicios disponibles a través de un sitio o sistema de información;

j) Correo electrónico: medio de intercambio de mensajes electrónicos en una dirección específica entre más de una persona física o jurídica a través de una red de información u otros medios electrónicos de interconexión, computadoras y similares;

k) Interceptación: la visualización u obtención de datos o información con el fin de fisgar, inutilizarlos, almacenarlos, copiarlos, grabarlos, modificar su contenido, utilizarlos indebidamente, desviarlos o redirigirlos con fines ilícitos;

l) Penetración: acceso a un sistema de información, una computadora, una red de información, etc. que no está autorizado, viola las disposiciones de la licencia correspondiente o es ilegal;

m) Contenido: cualquier dato que, por sí mismo o combinado con otros datos o información, conduzca a la formación de información o a la determinación de una tendencia, dirección, concepto o significado o referencia a otros datos;

n) Prueba digital: cualquier información probatoria electrónica que se almacena o transmite, se extrae u obtiene de computadoras, redes de información, etc. y que puede ser recogida y analizada mediante dispositivos tecnológicos especiales, programas o aplicaciones;

o) Tráfico (datos de tráfico): datos que produce un sistema de información y que muestran el origen, el destino, el remitente, el destinatario, la ruta, la hora, la fecha, el tamaño y la duración de una comunicación y el tipo de servicio.

Artículo 3. Protección de la soberanía

1. Los Estados partes cumplirán las obligaciones que les incumben en virtud de la presente Convención de conformidad con su derecho interno o sus principios constitucionales, de forma compatible con los principios de igualdad soberana de los Estados y de no injerencia en los asuntos internos de otros Estados.

2. La presente Convención no facultará a ningún Estado parte para ejercer, en el territorio de otro Estado, jurisdicción o funciones que el derecho interno de ese Estado reserve exclusivamente a sus autoridades.

Artículo 4. Ámbito de aplicación

1. Salvo que se disponga lo contrario, la presente Convención deberá aplicarse a la supresión de los delitos que se contemplen en ella.

2. A los efectos de la aplicación de esta Convención, no será necesario que los delitos u otros actos ilícitos contemplados en ella ocasionen daños materiales, salvo cuando se disponga lo contrario en ella.

3. Cada Estado parte considerará la posibilidad de limitar su reserva para permitir la amplia aplicación de las medidas mencionadas.

El Salvador

[Original: español]
[12 de abril de 2022]

Terminología

A consideración de nuestro Gobierno, existen varias definiciones que deben ser incorporadas dentro del documento y dichas definiciones deben contemplar los vocablos adecuados para que las traducciones a los seis idiomas oficiales de las Naciones Unidas trasladen los conceptos correctos sin que haya duda sobre el concepto al cual se quiere hacer referencia. Para este propósito se propone que el Comité Especial considere las definiciones ya establecidas en algunos instrumentos conocidos por los Estados Miembros, como el Convenio de Budapest y la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, como insumos que den comienzo para formular las definiciones.

Particularmente creemos que deben agregarse definiciones de los siguientes términos:

a) Por “sistema informático” se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa;

b) Por “datos informáticos” se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una acción;

c) Por “proveedor de servicios” se entenderá toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicarse a través de un sistema informático, y cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios de este;

d) Por “datos relativos al tráfico” se entenderá todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

Agregar la definición de “material con contenido de abuso infantil” en lugar de “pornografía infantil”, siendo los verbos rectores el producir, reproducir, distribuir, publicar, importar, exportar, ofrecer, financiar, vender, comercializar, difundir y poseer dichos contenidos y que esta definición incluya la participación de una persona que aparenta ser menor de edad en actos sexuales explícitos o imágenes realistas de una persona menor de edad que participa en actos sexuales explícitos, así como considerar en la definición no solo la exposición en actos sexualmente explícitos sino también aquellos actos que expongan la integridad física en desnudez de los niños, las niñas y adolescentes.

Unión Europea y sus Estados miembros

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

Capítulo I. Disposiciones generales

Artículo 1
Finalidad

Al tiempo que garantiza un alto nivel de protección de los derechos humanos y las libertades fundamentales, los propósitos de esta Convención son:

a) promover y fortalecer las medidas para prevenir y combatir más eficaz y eficientemente la ciberdelincuencia;

b) promover y facilitar la cooperación internacional;

c) asegurar un alto nivel de protección de los derechos de las víctimas, y

d) apoyar la creación de capacidad y la asistencia técnica en la lucha contra la ciberdelincuencia.

Artículo 2
Definiciones

A los efectos de la presente Convención:

a) Por "autoridad central" se entenderá una o varias autoridades encargadas de enviar las solicitudes de asistencia mutua o de responder a ellas, de ejecutarlas o de remitirlas a las autoridades competentes para su ejecución;

b) Por "ciberdelincuencia" se entenderá, a los efectos de esta Convención, las conductas definidas en los artículos 5 a 10 de la presente Convención;

c) Por "autoridad competente" se entenderá una autoridad judicial, administrativa o de otro tipo encargada de hacer cumplir la ley que esté facultada por el derecho interno para ordenar, autorizar o emprender la ejecución de medidas en virtud de la presente Convención con respecto a investigaciones o procedimientos penales específicos;

d) Por "sistema informático" se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa;

e) Por "datos informáticos" se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función;

f) Por "datos personales" se entenderá cualquier información relativa a una persona física identificada o identificable;

g) Por "organización regional de integración económica" se entenderá una organización constituida por Estados soberanos de una región determinada, a la que sus Estados miembros han transferido competencia en las cuestiones regidas por la presente Convención y que ha sido debidamente facultada, de conformidad con sus procedimientos internos, para firmar, ratificar, aceptar o aprobar la Convención o adherirse a ella; las referencias a los "Estados partes" con arreglo a la presente Convención se aplicarán a esas organizaciones dentro de los límites de su competencia;

h) Por "proveedor de servicios" se entenderá:

i) toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático, y

ii) cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para sus usuarios;

i) Por “datos relativos a los abonados” se entenderá cualquier información, en forma de datos informáticos o de cualquier otro modo, que posea un proveedor de servicios y que se refiera a los abonados de sus servicios, diferentes de los datos relativos al tráfico o al contenido, y que permitan determinar:

i) el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el período de servicio;

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

iii) cualquier otra información sobre el equipo de comunicaciones y el lugar donde esté instalado, disponibles en virtud de un contrato o de un acuerdo de prestación de servicio;

j) Por “datos relativos al tráfico” se entenderá todos los datos informáticos relativos a una comunicación realizada por medio de un sistema informático, generados por un sistema de este tipo en tanto que elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente;

k) Por “sin derecho” se entenderá una conducta mencionada en los artículos 5 a 10 de la presente Convención que no esté autorizada por el propietario o por otro titular de derechos del sistema informático o de una parte de él, o que no esté permitida por el derecho interno.

Artículo 3
Ámbito de aplicación

La presente Convención se aplicará, salvo que se indique lo contrario, a:

a) la prevención, la investigación y el enjuiciamiento de las infracciones penales establecidas de conformidad con los artículos 5 a 10 de la Convención;

b) la obtención de pruebas en forma electrónica de una infracción penal establecida de conformidad con los artículos 5 a 10 de la presente Convención sobre la base de las medidas establecidas en el capítulo III de la Convención;

c) el suministro y la prestación de asistencia técnica y el desarrollo de capacidades en los asuntos cubiertos por esta Convención.

Artículo 4
Efectos de la Convención

1. Si dos o más Estados partes han celebrado ya un acuerdo o un tratado relativo a las cuestiones contempladas en la presente Convención, o han regulado de otro modo sus relaciones al respecto, o si lo hacen en el futuro, podrán asimismo aplicar el citado acuerdo o tratado, o regular sus relaciones de conformidad con él. No obstante, cuando los Estados partes regulen sus relaciones futuras respecto de las cuestiones objeto de la presente Convención de forma distinta a la prevista en ella, lo harán de modo que no sea incompatible con los objetivos y principios de la Convención.

2. Con respecto a los Estados partes que sean miembros de una organización regional de integración económica, estos podrán aplicar, en sus relaciones mutuas, las normas de esa organización regional de integración económica que rijan las cuestiones tratadas en la presente Convención.

3. Nada de lo dispuesto en la presente Convención afectará a otros derechos, restricciones, obligaciones y responsabilidades de cada parte en virtud del derecho internacional, en particular el derecho de los derechos humanos.

Ghana

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

Capítulo I. Disposiciones generales

Artículo 1
Finalidad

La finalidad de la presente Convención es promover y facilitar la cooperación internacional, así como reforzar las medidas para prevenir y combatir el uso de las tecnologías de la información y las comunicaciones con fines delictivos.

Artículo 2
Definiciones

A los efectos de la presente Convención:

a) Por “sistema informático” se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa;

b) Por “datos informáticos” se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función;

c) Por “datos de contenido” se entenderá el contenido de la comunicación, es decir, el significado o el propósito de la comunicación o el mensaje o la información que transmite la comunicación, con excepción de los datos de tráfico;

d) Por “niño” se entenderá una persona menor de 18 años. Las partes podrán, no obstante, exigir un límite de edad inferior, que deberá ser como mínimo de 16 años;

e) Por “infraestructura crítica de información” se entenderá una computadora o sistema informático que un Estado Miembro defina en su derecho interno como esencial para la seguridad nacional o el bienestar económico y social de los ciudadanos;

f) El “registro prohibido visual y de imágenes íntimas” incluye:

i) imágenes en movimiento o fijas que representen:

a. a una persona que participa en una actividad sexual íntima que no se realiza habitualmente en público, o

b. la zona genital o anal de una persona, cuando esta zona está desnuda o cubierta solo por ropa interior; y

ii) una imagen que ha sido alterada para que parezca mostrar cualquiera de las cosas mencionadas en el párrafo i), incluso si el objeto de la imagen ha sido ocultado por medios digitales, si la persona es representada de manera sexual;

g) Por “proveedor de servicios” se entenderá:

i) toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicarse a través de un sistema informático, y

ii) cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para sus usuarios;

h) Por “abonado” se entenderá un cliente o usuario de una red de comunicaciones electrónicas, de un servicio de comunicaciones electrónicas o de un servicio de radiodifusión;

i) Por “información relativa a los abonados” se entenderá cualquier información, en forma de datos informáticos o de cualquier otro modo, que posea un

proveedor de servicios y que se refiera a los abonados de sus servicios, diferentes de los datos relativos al tráfico o al contenido, y que permitan determinar:

i) el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el período de servicio;

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

iii) cualquier otra información relativa al lugar en que se encuentren los equipos de comunicación, disponible en virtud de un contrato o de un acuerdo de prestación de servicio;

j) Por "datos relativos al tráfico" se entenderá todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

Artículo 3
Ámbito de aplicación

La presente Convención se aplicará, de conformidad con sus disposiciones, a:

a) la prevención, la investigación y el enjuiciamiento de los delitos establecidos de conformidad con los artículos 5 a 20;

b) la obtención de pruebas electrónicas de cualquier delito;

c) el suministro y la prestación de asistencia técnica y el desarrollo de capacidades en los asuntos comprendidos en esta Convención;

d) el embargo preventivo, la incautación, el decomiso y la restitución del producto de delitos tipificados con arreglo a la presente Convención.

Artículo 4
Protección de la soberanía

1. Los Estados partes 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 Miembro para ejercer, en el territorio de otro Estado, jurisdicción o funciones que el derecho interno de ese Estado reserve exclusivamente a sus autoridades.

Irán (República Islámica del)

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

1. Disposiciones generales

A pesar de las excepcionales oportunidades que ofrecen las tecnologías de la información y las comunicaciones para el desarrollo de las naciones, los delincuentes están haciendo un enorme uso indebido de dichas tecnologías para llevar a cabo actividades ilícitas y alcanzar fines ilegítimos. El *modus operandi* de estos delincuentes se está volviendo cada vez más diverso y sofisticado y el carácter compuesto de estos delitos está evolucionando sustancialmente. Los delitos cometidos mediante el uso de las tecnologías de la información y las comunicaciones a menudo superan las fronteras geográficas, lo que los convierte en un reto acuciante sin precedentes para los Estados

Miembros. Por ello, es más que necesario fortalecer la respuesta colectiva y la cooperación a nivel internacional dentro de un marco jurídico internacional sólido.

El Comité Especial fue creado por la Asamblea General en virtud de su resolución 74/247 con el fin de responder a esta necesidad urgente y elaborar un instrumento jurídico internacional en que se sustentaran medidas eficaces a diversos niveles para combatir el uso de las tecnologías de la información y las comunicaciones con fines delictivos. Para ello, en las disposiciones generales de la convención deberían estipularse sus propósitos y definirse su ámbito de aplicación. Como práctica establecida y dada la importancia subyacente del cumplimiento de los principios fundamentales del derecho internacional en la prevención y la lucha contra los delitos cometidos mediante el uso de las tecnologías de la información y las comunicaciones, también debería dedicarse una sección sustantiva a dichos principios en las disposiciones generales. Definir la terminología utilizada en la convención en una sección específica es esencial para asegurar la comprensión común de los términos importantes y, en última instancia, de las disposiciones del instrumento.

1.1 Objetivos de la convención

Teniendo en cuenta lo mencionado, la República Islámica del Irán pone de relieve que la convención debería tener como objetivo reforzar, apoyar y facilitar la cooperación internacional para prevenir y combatir el uso de las tecnologías de la información y las comunicaciones con fines delictivos, incluida la recuperación de activos, fortalecer las respuestas nacionales a estos delitos y ayudar a los Estados partes, en particular a los países en desarrollo, a luchar contra estos delitos, entre otras cosas, mediante el desarrollo económico, la prestación de asistencia técnica y la transferencia de tecnología. A este respecto, los retos y barreras, como las sanciones unilaterales y el subdesarrollo, que socavan la capacidad de los Estados para combatir eficazmente el uso de las tecnologías de la información y las comunicaciones con fines delictivos deben afrontarse en un contexto técnico.

También debe tenerse debidamente en cuenta la responsabilidad de los proveedores de servicios y otras entidades similares en la cooperación con las autoridades judiciales y encargadas de hacer cumplir la ley para garantizar medidas eficaces de prevención y lucha contra el uso de las tecnologías de la información y las comunicaciones con fines delictivos.

Mientras que una comprensión común del fenómeno delictivo y de sus cambiantes formas es de suma importancia para responder eficazmente a los delitos cometidos a través de las tecnologías de la información y las comunicaciones, la convención también debería promover y facilitar el intercambio de información, conocimientos técnicos y especializados, experiencias y buenas prácticas.

Dichos objetivos se harán realidad si se adopta un enfoque que valore un futuro compartido en el ciberespacio para todos los Estados Miembros, con igualdad de oportunidades y sin discriminación.

1.2 Ámbito de aplicación de la convención

La convención debería incluir en su ámbito de aplicación los delitos que dependen de las tecnologías de la información y las comunicaciones, como los delitos contra la confidencialidad y la integridad de los sistemas y datos informáticos y los delitos contra las infraestructuras de las tecnologías de la información y las comunicaciones, así como los que son facilitados por estas tecnologías, por ejemplo, los insultos a los valores religiosos, la incitación a la violencia o a cometer homicidios, la distribución de contenidos delictivos y obscenos y la explotación sexual de niños. No obstante, los delitos facilitados por las tecnologías de la información y las comunicaciones pueden requerir un enfoque individualizado que tenga en cuenta los distintos factores que rodean a las diversas formas de delitos y las posibles diferencias en los elementos del delito necesarios para definirlos como tales. En su caso, también pueden ser necesarios otros elementos para definir el ámbito de aplicación de la convención en función de la

gravedad o las penas de los delitos y teniendo en cuenta si los delitos en cuestión se han perpetrado en más de un Estado.

1.3 Protección de la soberanía

La República Islámica del Irán reafirma que deben incluirse en las disposiciones generales artículos referidos específicamente a la protección de la soberanía para garantizar que los esfuerzos y las medidas de prevención y lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos sean coherentes y se ajusten a los principios fundamentales del derecho internacional y a los principios establecidos en la Carta de las Naciones Unidas, en particular, la igualdad de soberanía, la integridad territorial de los Estados y la no intervención. Esta es una práctica establecida en la elaboración de instrumentos en el ámbito de la prevención y la lucha contra los delitos; por ejemplo, el término “protección de la soberanía” se ha empleado en instrumentos como la Convención de las Naciones Unidas contra la Corrupción.

La República Islámica del Irán se mantiene circunspecta ante los intentos que van en contra de esta práctica establecida de la comunidad internacional y pretenden negar e ignorar el papel esencial de la conformidad con estos principios en la lucha contra la delincuencia.

Japón

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

2. Disposiciones generales

2.1 Finalidad

Apoyamos los tres objetivos esbozados en la propuesta presentada por la Presidenta en el primer período de sesiones del Comité Especial, a saber: a) promover y reforzar las medidas para prevenir y combatir la ciberdelincuencia; b) promover, facilitar y reforzar la cooperación internacional, y c) proporcionar herramientas prácticas para mejorar la asistencia técnica y desarrollar la capacidad de las autoridades nacionales.

2.2 Definiciones

Desde el punto de vista de la creación de una convención que se utilizará eficazmente durante un largo período de tiempo, los términos utilizados en ella deben estar claramente definidos de manera tecnológicamente neutra. Por ejemplo, no sería conveniente incluir definiciones referidas a tecnologías que cambian constantemente, como “red de bots”.

Por lo tanto, las definiciones deben establecerse de la manera más general y clara posible y en la medida necesaria, haciendo referencia a los instrumentos internacionales existentes, como la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional. Creemos que esta perspectiva es igualmente válida para los debates sobre otras partes de esta convención, como las disposiciones sobre criminalización.

2.3 Ámbito de aplicación

2.3.1. El ámbito de aplicación de esta convención debe estar claramente establecido en base a las disposiciones de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y de la Convención de las Naciones Unidas contra la Corrupción.

2.3.2. No deben incluirse en esta convención la ciberseguridad ni la gobernanza de Internet. Por ejemplo, las siguientes medidas tendrían un efecto de enfriamiento de la

actividad económica legítima, obstaculizarían el desarrollo de la tecnología e irían más allá del mandato del Comité Especial:

- establecer normas de seguridad en el marco de esta convención;
- imponer a las personas jurídicas y físicas la obligación de cumplir dichas normas o imponer sanciones por su incumplimiento, o
- responsabilizar a las personas jurídicas, a sus representantes o a los creadores de programas informáticos que hayan participado involuntariamente en ciberdelitos cometidos por otros actores sin su conocimiento.

México

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

Disposiciones generales

Para evitar posibles omisiones e incumplimientos en la aplicación de otros instrumentos jurídicamente vinculantes en el futuro, y de acuerdo con los tratados internacionales y regionales precedentes, México es partidario de que se incluyan en las disposiciones iniciales referencias generales, en lugar de otras muy exhaustivas y detalladas.

En cuanto a la soberanía, y siguiendo el ejemplo de la Convención Marco de las Naciones Unidas sobre el Cambio Climático, México recomienda que se incluya desde el preámbulo una referencia general dirigida a reafirmar la soberanía que rece: "Reafirmando el principio de la soberanía de los Estados en la cooperación internacional para hacer frente a la utilización de las tecnologías de la información y las comunicaciones con fines delictivos".

México también recomienda que se incluya un párrafo en el preámbulo en el que se reafirmen la Carta de las Naciones Unidas, la aplicabilidad del derecho internacional y la Declaración Universal de los Derechos Humanos y otras obligaciones en materia de derechos humanos, como sigue: "Reafirmando los propósitos y principios de la Carta de las Naciones Unidas, el derecho internacional y la Declaración Universal de Derechos Humanos y otros instrumentos pertinentes en materia de derechos humanos".

También se recomienda incluir una disposición general sobre la importancia de que los Estados adopten medidas adecuadas para proteger a las personas y, en particular, a los grupos vulnerables: "Decidida a adoptar medidas de prevención, respuesta, mitigación, investigación y enjuiciamiento para proteger eficazmente a las personas y, en particular, a los grupos vulnerables del uso de las tecnologías de la información y las comunicaciones con fines delictivos".

Como ya se dijo en esta propuesta, para el Gobierno de México será esencial que se tengan en cuenta a lo largo de la convención las medidas de prevención, respuesta, mitigación, investigación y persecución.

Durante el proceso de negociación de la convención será importante reconocer la relevancia de los instrumentos internacionales jurídicamente vinculantes anteriores, en particular la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, y aportar experiencias concretas que podrían utilizarse para hacer más eficiente la cooperación internacional en la lucha contra los delitos cibernéticos. Debe incluirse como disposición general un llamamiento a promover la coherencia de todo el sistema de las Naciones Unidas a este respecto.

México recomienda que se incluya también en el preámbulo un reconocimiento explícito de las oportunidades y beneficios que aportan las tecnologías de la información y las comunicaciones para dejar claro que no son utilizadas exclusivamente con fines delictivos e ilícitos: "Reconociendo que las tecnologías de la información, las telecomunicaciones y las tecnologías digitales brindan oportunidades para potenciar el

desarrollo, cerrar las brechas de desigualdad y promover la inclusión, el bienestar, la justicia y el ejercicio de los derechos humanos, y reconociendo la importancia de fomentar el acceso universal a estas tecnologías y de proteger los beneficios que conllevan".

Además, México comparte su interés por evitar caer en el uso excesivo de salvaguardas que puedan actuar como una restricción, lo que contraría el espíritu de cooperación internacional que debe orientar este proceso.

"La finalidad de la presente Convención es promover la cooperación bilateral y multilateral y la asistencia jurídica, incluida la cooperación multisectorial, en la prevención, investigación, mitigación y enjuiciamiento de la utilización de las tecnologías de la información y las comunicaciones con fines delictivos y la respuesta a ella".

México considera que deben añadirse otras disposiciones generales sobre los siguientes temas: definición de los procedimientos de solución de conflictos; establecimiento de un mecanismo de examen de la aplicación; participación y colaboración de otras partes interesadas en el apoyo a los esfuerzos realizados por los Estados partes para prevenir y combatir el uso de las tecnologías de la información y las comunicaciones con fines delictivos; reconocimiento del núcleo público de Internet y la relevancia del enfoque de la neutralidad de la red para los fines de la Convención.

Nueva Zelandia

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

Disposiciones generales

8. En nuestra opinión, las disposiciones generales deberían consistir en:

- *Finalidad*. La mejor manera de elaborar un tratado eficaz es adoptar un enfoque coherente, realista y centrado en la determinación de nuestros objetivos. En opinión de Nueva Zelandia, el objetivo debería ser establecer un marco mundial armonizado, moderno y eficaz de cooperación y coordinación entre los Estados para afrontar la amenaza cada vez más grave que supone la ciberdelincuencia para las personas, las empresas y los Gobiernos. Esto incluye la prestación de apoyo y asistencia técnica a fin de que todos los Estados desarrollen la capacidad y las aptitudes para hacer frente a esos desafíos.
- *Ámbito de aplicación*. Asimismo, el ámbito de aplicación debería ser específico y estar claramente definido. La propuesta de la Presidenta, que figura en el documento de sesión A/AC.291/CRP.8/Rev.1, proporciona una buena base para determinar el alcance de la convención.
- *Definiciones acordadas*. Las definiciones deben ser precisas e inequívocas, no quedar obsoletas en el futuro y, en la medida de lo posible, estar basadas en los instrumentos internacionales y regionales existentes.
- Un instrumento integral debe incluir también una disposición general que haga hincapié en la protección de los derechos humanos y las libertades fundamentales y en el respeto del estado de derecho, teniendo especialmente en cuenta las perspectivas de las mujeres, los niños, los pueblos indígenas y los grupos vulnerables.

9. Varios Estados también han manifestado que es importante para ellos que se incluya una disposición relativa a la soberanía de los Estados. Señalamos que la aplicación de cualquier disposición de este tipo en el contexto de esta convención debe tener en cuenta algunas características críticas que distinguen el ciberespacio del ámbito físico, en particular las siguientes: a) el ciberespacio contiene un elemento virtual que no tiene un vínculo territorial claro, y b) la actividad cibernética puede implicar

infraestructuras cibernéticas que funcionen simultáneamente en múltiples territorios y jurisdicciones difusas.

Anexo II
Definiciones

Por “sistema informático” se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.

Por “datos informáticos” se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que una computadora ejecute una función tal.

Por “imágenes de explotación sexual de niños” se entenderá todo material, incluidas imágenes, videos o transmisiones en vivo, que represente de forma visual a un niño que mantenga una conducta sexualmente explícita, real o simulada, o toda representación de un niño con fines principalmente sexuales.

Por “bienes” se entenderá los activos de cualquier tipo, incluidos los digitales, corporales o incorporales, muebles o inmuebles, tangibles o intangibles, y los documentos o instrumentos legales que acrediten la propiedad u otros derechos sobre dichos activos.

Noruega

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

Disposiciones generales

1. La convención debería incluir disposiciones sólidas sobre la protección de los derechos humanos y las libertades fundamentales, incluido el derecho a la privacidad y la protección de los datos personales. Debemos garantizar la plena compatibilidad de una futura convención de las Naciones Unidas sobre la ciberdelincuencia con las obligaciones jurídicas internacionales en este ámbito.

2. Para ser eficaz, este instrumento debe proporcionar las garantías necesarias, entre ellas la proporcionalidad, la legalidad y la necesidad de la acción de los organismos encargados de hacer cumplir la ley.

3. La finalidad debe centrarse en la cooperación internacional para prevenir y combatir la ciberdelincuencia.

Federación de Rusia, también en nombre de Belarús, Burundi, China, Nicaragua y Tayikistán

[Original: ruso]
[7 de abril de 2022]

Capítulo I. Disposiciones generales

Artículo 1. Objetivos

Los objetivos de la presente Convención son:

a) Promover la adopción y el fortalecimiento de medidas para prevenir y combatir eficazmente los delitos relacionados con las tecnologías de la información y las comunicaciones y otros actos ilícitos;

b) Prevenir las acciones que atenten contra la confidencialidad, la integridad y la disponibilidad de las tecnologías de la información y las comunicaciones, y prevenir el uso indebido de estas tecnologías, tipificando como delito los actos contemplados en

esta Convención y proporcionando las facultades suficientes para combatir con eficacia dichos delitos y otros actos ilícitos, facilitando su detección, investigación y enjuiciamiento tanto a nivel nacional como internacional y desarrollando acuerdos de cooperación internacional;

c) Mejorar la eficacia de la cooperación internacional y desarrollarla, incluso en el ámbito de la capacitación y la prestación de asistencia técnica para prevenir y combatir los delitos relacionados con las tecnologías de la información y las comunicaciones.

Artículo 2. Ámbito de aplicación

1. La presente Convención se aplicará, de conformidad con sus disposiciones, a la prevención, detección, supresión, investigación y enjuiciamiento de los delitos y otros actos ilícitos reconocidos como tales en virtud de los artículos 6 a 29 de la presente Convención y a la aplicación de medidas para eliminar las consecuencias de dichos actos, incluida la suspensión de las transacciones relativas a los activos obtenidos de resultas de la comisión de cualquier delito u otro acto ilícito tipificado como tal en la presente Convención, así como la incautación, el decomiso y la restitución del producto de tales delitos.

2. A los efectos de la aplicación de esta Convención, no será necesario que los delitos u otros actos ilícitos contemplados en ella ocasionen daños materiales, salvo que se disponga lo contrario en ella.

Artículo 3. Protección de la soberanía

1. Los Estados partes cumplirán las obligaciones que les incumben en virtud de la presente Convención de conformidad con los principios de soberanía del Estado, igualdad soberana de los Estados y no injerencia en los asuntos internos de otros Estados.

2. La presente Convención no facultará a las autoridades competentes de un Estado parte para ejercer en el territorio de otro Estado parte la jurisdicción y las funciones que el derecho interno de ese Estado reserve exclusivamente a sus autoridades, salvo que se disponga en ella lo contrario.

Artículo 4. Términos y definiciones

A los efectos de la presente Convención:

a) Por “incautación de bienes” se entenderá la prohibición temporal de transferir, convertir, enajenar o trasladar bienes, o la asunción temporal de la custodia o el control de bienes sobre la base de una orden de un tribunal u otra autoridad competente;

b) Por “red de bots” se entenderá dos o más dispositivos de tecnologías de la información y las comunicaciones en los que se han instalado programas maliciosos y que se controlan de forma centralizada sin el conocimiento de los usuarios;

c) Por “programa malicioso” se entenderá *software* cuya finalidad es la modificación, destrucción, copia y bloqueo no autorizados de información, o la neutralización del *software* utilizado para la seguridad de la información digital;

d) “Pornografía infantil” tendrá el significado que se asigna a este término en el artículo 2 c) del 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, de 25 de mayo de 2000;

e) Por “producto” se entenderá los bienes de cualquier índole derivados u obtenidos directa o indirectamente de la comisión de un delito u otro acto ilícito contemplado en la presente Convención, así como los ingresos u otros beneficios derivados de ese producto del delito, los bienes en los que se haya transformado o

convertido dicho producto o los bienes con los que se haya entremezclado ese producto del delito;

f) Por “tecnologías de la información y las comunicaciones” se entenderán los procesos y métodos de generación, tratamiento y distribución de la información, así como las formas y medios para implementarlos;

g) Por “redes de información y telecomunicaciones” se entenderá un conjunto de equipos de ingeniería destinados a controlar los procesos tecnológicos mediante la tecnología informática y las telecomunicaciones;

h) Por “bienes” se entenderá 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 sobre dichos activos o una parte de ellos;

i) Por “información” se entenderá cualquier dato (mensajes, registros), independientemente de la forma en que se presente;

j) Por “decomiso” se entenderá la privación forzosa de bienes sin compensación en virtud de una orden de un tribunal u otra autoridad competente;

k) Por “ataque informático” se entenderá la interferencia selectiva de *software* o *hardware* y *software* con sistemas de información o redes de información y telecomunicaciones para interrumpir y/o poner fin a su funcionamiento y/o amenazar la seguridad de la información procesada por dichas instalaciones;

l) Por “información digital” se entenderá cualquier dato (registro), independientemente de su forma y características, contenido y procesado en dispositivos, sistemas y redes de información y telecomunicaciones;

m) Por “infraestructura de información crítica” se entenderá un conjunto de instalaciones de infraestructura de información crítica y redes de telecomunicaciones utilizadas para interconectar las instalaciones de infraestructura de información crítica;

n) Por “instalaciones de infraestructura crítica” se entenderá los sistemas de información y las redes de información y comunicaciones de las autoridades públicas, así como los sistemas de información y los sistemas de control de procesos automatizados de los sectores de la defensa, la sanidad, la educación, el transporte, las comunicaciones, la energía, la banca y las finanzas, la energía nuclear y otros ámbitos importantes de la vida del Estado y de la sociedad;

o) Por “proveedor de servicios” se entenderá:

i) toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicarse a través de las tecnologías de la información y las comunicaciones, o

ii) cualquier otra entidad que procese o almacene información electrónica en nombre de una entidad mencionada en el apartado i) o de los usuarios de los servicios prestados por dicha entidad;

p) Por “datos de tráfico” se entenderá cualquier información electrónica (excluyendo el contenido de los datos transferidos) relativa a la transferencia de datos por medio de las tecnologías de la información y las comunicaciones y que indique, en particular, el origen, el destino, la ruta, la hora, la fecha, el tamaño, la duración y el tipo de servicio de red subyacente;

q) Por “dispositivo de tecnologías de la información y las comunicaciones” se entenderá un conjunto (agrupación) de componentes de *hardware* utilizados o diseñados para el procesamiento automático, el almacenamiento y la transferencia de información electrónica;

r) Por “prueba electrónica” se entenderá cualquier información probatoria almacenada o transmitida en forma digital (en un soporte electrónico).

El término “daño sustancial” se determinará de acuerdo con el derecho interno del Estado parte requerido.

Sudáfrica

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

Capítulo I. Disposiciones generales

Artículo 1. Declaración de objetivos

Los objetivos de la Convención han de ser:

a) promover y fortalecer las medidas para prevenir y combatir la utilización de las tecnologías de la información y las comunicaciones con fines delictivos/la ciberdelincuencia, protegiendo al mismo tiempo de tales delitos a los usuarios de estas tecnologías;

b) promover y fortalecer las medidas destinadas a prevenir y combatir eficazmente los delitos y otros actos ilícitos en el ámbito de las tecnologías de la información y las comunicaciones;

c) promover, facilitar y apoyar la cooperación internacional para prevenir y combatir la utilización de las tecnologías de la información y las comunicaciones con fines delictivos/la ciberdelincuencia;

d) proporcionar herramientas prácticas para mejorar la asistencia técnica entre los Estados partes y fomentar la capacidad de las autoridades nacionales para prevenir y combatir el uso de las tecnologías de la información y las comunicaciones con fines delictivos/la ciberdelincuencia y fortalecer las medidas para promover el intercambio de información, experiencias y buenas prácticas.

Artículo 2. Términos empleados

A los efectos de la presente Convención:

a) Se entenderá por “artículo” todo:

i) dato;

ii) programa informático;

iii) soporte de almacenamiento de datos informáticos, o

iv) sistema informático

que:

a. esté relacionado o conectado con la comisión o sospecha de comisión, o se crea, por motivos razonables, que está relacionado o conectado con la comisión o sospecha de comisión;

b. pueda aportar pruebas de la comisión o de la sospecha de comisión, o

c. esté destinado a ser utilizado o se crea, por motivos razonables, que está destinado a ser utilizado en la comisión o en la intención de comisión, de:

i. un delito tipificado en esta Convención;

ii. cualquier otro delito perpetrado mediante la utilización de las tecnologías de la información y las comunicaciones, o

iii. un delito en un Estado extranjero que sea similar en lo sustantivo a un delito contemplado en la presente Convención;

b) Por “material que muestra abusos sexuales de niños” se entenderá cualquier imagen, independientemente de cómo se haya creado, o cualquier descripción o

presentación, incluida cualquier fotografía, película, video, imagen, ya sea realizada o producida por medios electrónicos, mecánicos o de otro tipo, de una conducta sexualmente explícita, cuando:

i) la producción de esta representación visual implique a un menor;

ii) dicha representación visual sea una imagen digital, una imagen de computadora o una imagen generada por computadora en la que un menor participe en una conducta sexualmente explícita o cuando se produzcan o utilicen imágenes de sus órganos sexuales con fines principalmente sexuales y se exploten con o sin el conocimiento del niño, y

iii) dicha representación visual haya sido creada, adaptada o modificada para que parezca que un niño está participando en una conducta sexualmente explícita;

c) Por “computadora” se entenderá cualquier dispositivo electrónico programable que se utilice, ya sea por sí mismo o como parte de un sistema informático o cualquier otro dispositivo o equipo, o cualquier parte de él, para realizar operaciones aritméticas, lógicas, de enrutamiento, de procesamiento o de almacenamiento predeterminadas de acuerdo con instrucciones establecidas, e incluye cualquier dato, programa informático o soporte de almacenamiento de datos informáticos que estén relacionados con dicho dispositivo, conectados a él o utilizados junto con él;

d) Por “datos informáticos” se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función;

e) Por “soporte de almacenamiento de datos informáticos” se entiende cualquier dispositivo desde el que se puedan reproducir datos o un programa informático o en el que se puedan almacenar datos o un programa informático, mediante un sistema informático, independientemente de que el dispositivo esté físicamente unido o conectado a un sistema informático;

f) Por “programa informático” se entenderán datos que representan instrucciones que, cuando se ejecutan en un sistema informático, hacen que este realice una función;

g) Por "sistema informático" se entenderá:

i) una computadora, o

ii) dos o más computadoras interconectadas o relacionadas entre sí, de modo que permita que estas computadoras:

a. intercambien datos o cualquier otra función entre ellas, o

b. intercambien datos o cualquier otra función con otra computadora o sistema informático;

h) Por “decomiso” se entenderá la privación con carácter definitivo de bienes por decisión de un tribunal o de otra autoridad competente;

i) Por “delito basado en la cibernética” se entenderá un delito que solo se puede cometer utilizando una computadora, redes informáticas u otro tipo de tecnología de la información y las comunicaciones;

j) Por “delito facilitado por la cibernética” se entenderá un que no depende de computadoras o redes, pero cuya magnitud o la forma que adopta se ha visto modificada por el uso de Internet y la tecnología de las comunicaciones;

k) Por “mensaje de datos” se entenderá los datos generados, enviados, recibidos o almacenados por medios electrónicos, cuando la salida de datos tiene un formato inteligible;

l) Por “información digital” se entenderá todo dato (registro), independientemente de su forma y características, contenido y procesado en dispositivos, sistemas y redes de información y comunicación;

m) Por “prueba electrónica” se entenderá toda información probatoria almacenada o transmitida en forma digital (en un soporte electrónico);

n) Por “embargo preventivo” se entenderá la prohibición temporal de transferir, convertir, enajenar o mover bienes, o la custodia o el control temporales de bienes por mandamiento expedido por un tribunal u otra autoridad competente;

o) Por “bienes” se entenderá los activos de cualquier tipo, corporales o incorporales, muebles o inmuebles, tangibles o intangibles, y los documentos o instrumentos legales que acrediten la propiedad u otros derechos sobre dichos activos;

p) Por “producto del delito” se entenderá los bienes de cualquier índole derivados u obtenidos directa o indirectamente de la comisión de un delito;

q) Por “delito determinante” se entenderá todo delito del que se derive un producto que pueda pasar a constituir materia de un delito definido en el artículo 23 de la presente Convención y el derecho interno del Estado parte/Estado Miembro;

r) Por “incautación de activos” se entenderá la toma de control permanente de los activos o de la custodia o el control temporales de bienes por mandamiento expedido por un tribunal u otra autoridad competente;

s) Por “proveedor de servicios” se entenderá cualquier entidad pública o privada que proporcione a los usuarios de su servicio la posibilidad de comunicarse mediante un sistema informático, o cualquier otra entidad que procese o almacene datos informáticos en nombre de dicho servicio de comunicación o de los usuarios de dicho servicio;

t) Por “datos de tráfico” se entenderá los datos relativos a una comunicación que indican el origen, el destino, la ruta, el formato, la hora, la fecha, el tamaño, la duración o el tipo de comunicación del servicio subyacente.

Artículo 3. Ámbito de aplicación

La presente Convención se aplicará, de conformidad con sus términos, a la prevención, la investigación y el enjuiciamiento de los delitos basados en la cibernética o determinados delitos facilitados por la cibernética que se hayan cometido mediante la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, así como al embargo preventivo, la incautación, el decomiso y la restitución del producto de los delitos tipificados con arreglo a esta Convención.

Artículo 4. Protección de la soberanía

1. Los Estados partes 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 Miembro para ejercer, en el territorio de otro Estado, jurisdicción o funciones que el derecho interno de ese Estado reserve exclusivamente a sus autoridades.

Suiza

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

2.1. Disposiciones generales

Finalidad

La finalidad de la presente Convención es:

a) promover y fortalecer las medidas para [prevenir/contrarrestar y combatir] más eficaz y eficientemente la ciberdelincuencia;

b) promover, facilitar y apoyar la cooperación internacional y la asistencia técnica en la prevención y la lucha contra la ciberdelincuencia.

Respeto y protección de los derechos humanos y las libertades fundamentales

Los Estados partes deben cumplir sus obligaciones con arreglo a la presente Convención de manera coherente con sus obligaciones en virtud del derecho internacional de los derechos humanos.

Definiciones

Por “sistema informático” se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.

Por “datos informáticos” se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.

Por “proveedor de servicios” se entenderá:

a) toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicarse a través de un sistema informático, y

b) cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para sus usuarios.

Por “datos relativos al tráfico” se entenderá todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

Ámbito de aplicación

A menos que contenga una disposición en contrario, la presente Convención se aplicará a la prevención, la investigación y el enjuiciamiento de los delitos establecidos de conformidad con las disposiciones relativas a la criminalización que contiene.

Reino Unido de Gran Bretaña e Irlanda del Norte

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

Capítulo. Disposiciones generales

Artículo 1. Propósito

El propósito de la presente Convención es promover la cooperación internacional y la asistencia técnica para prevenir y combatir la ciberdelincuencia.

Artículo 2. Definiciones

A los efectos de la presente Convención:

a) Por “sistema informático” se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa;

b) Por “datos informáticos” se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función;

c) Por “proveedor de servicios” se entenderá:

i) toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicarse a través de un sistema informático, y

ii) cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para sus usuarios.

d) Por “datos relativos al tráfico” se entenderá todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

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 establecidos en ella.

2. La presente Convención también puede aplicarse, cuando así se indique, a la obtención de pruebas en forma electrónica de un delito.

Artículo 4. Protección de los derechos humanos

Cada parte velará por que el cumplimiento de sus obligaciones con arreglo a la presente Convención se ajuste al derecho internacional de los derechos humanos.

Observaciones adicionales

El Reino Unido considera que también puede ser apropiado que en el capítulo relativo a las disposiciones generales se trate la forma en que esta convención se relaciona con otros instrumentos de justicia penal de las Naciones Unidas y los complementa, y que incluya un compromiso de incorporar una perspectiva de género en la aplicación de las disposiciones de la convención.

República Unida de Tanzanía

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

3. Disposiciones generales

La finalidad de la convención debería ser promover la cooperación en la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos. El mundo cibernético es cambiante y en este momento existe una amplia gama de terminologías utilizadas en las tecnologías de la información y las comunicaciones. Es imprescindible que la convención defina términos de aplicación universal en las tecnologías de la información y las comunicaciones para evitar ambigüedades o malentendidos.

3.1. Definiciones

La República Unida de Tanzania considera que la convención debe prever la definición de los términos pertinentes de manera tecnológicamente neutra para dar cabida a los rápidos cambios de la tecnología. Deberían incluirse los términos siguientes:

a) acceso;

b) proveedor de acceso;

c) proveedor de servicios de almacenamiento en caché;

d) niño;

e) utilización de niños en la pornografía;

f) sistema informático;

g) datos informáticos;

h) decomiso;

i) bienes de contrabando;

j) criptografía;

k) ciberterrorismo;

l) datos;

m) mensaje de datos;

n) soporte de almacenamiento de datos;

o) datos electrónicos;

p) embargo preventivo;

q) obstaculizar en relación con un sistema informático;

r) sistema de mensajes interactivos;

s) interceptación, en relación con una función informática;

t) interconexión;

u) remitente;

v) material racista y xenófobo;

w) incautación;

x) proveedor de servicios en relación con las tecnologías de la información y las comunicaciones;

y) datos de tráfico.

3.2. Jurisdicción

La convención debería prever las medidas legislativas y de otro tipo que sean necesarias para que cada Estado parte establezca su jurisdicción respecto de los delitos tipificados con arreglo a la convención cuando:

a) el delito se cometa en su territorio;

b) el delito se cometa a bordo de un buque que enarbole su pabellón o de una aeronave registrada conforme a sus leyes;

c) el delito se dirige contra un sistema, un dispositivo o datos informáticos o una persona situados en su territorio;

d) el delito se cometa por o contra uno de sus nacionales.

Estados Unidos de América

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

Definiciones

Por “niño” se entenderá toda persona menor de 18 años.

Por “material que muestra abusos sexuales de niños” se entenderá toda representación visual o transmisión en directo de: a) un niño que participa en una conducta sexualmente explícita real o simulada, o b) un adulto que participa en una conducta sexualmente explícita real o simulada con un niño incluido intencionadamente en la representación visual o transmisión en directo. No será necesario que el niño sea consciente o esté al tanto de la naturaleza de dicha conducta sexualmente explícita ni que pueda reconocerla[6].

Por “datos informáticos” se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que una computadora ejecute una función tal.

Por “sistema informático” se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.

Por “decomiso” se entenderá la privación con carácter definitivo de bienes por decisión de un tribunal o de otra autoridad competente[7].

Por “delitos cibernéticos” se entenderá los delitos establecidos de conformidad con la presente Convención.

Por “embargo preventivo” o “incautación” se entenderá la prohibición temporal de transferir, convertir, enajenar o mover bienes, o la custodia o el control temporales de bienes por mandamiento expedido por un tribunal u otra autoridad competente[8].

Por “delito determinante” se entenderá todo delito del que se derive un producto que pueda pasar a constituir materia de un delito definido en el artículo de la presente Convención relativo a la criminalización del blanqueo del producto de la ciberdelincuencia[9].

Por “producto del delito” se entenderá los bienes de cualquier índole derivados u obtenidos directa o indirectamente de la comisión de un delito[10].

Por “bienes” se entenderá los activos de cualquier tipo, corporales o incorporales, muebles o inmuebles, tangibles o intangibles, y los documentos o instrumentos legales que acrediten la propiedad u otros derechos sobre dichos activos[11].

Por “organización regional de integración económica” se entenderá una organización constituida por Estados soberanos de una región determinada, a la que sus Estados miembros han transferido competencia en las cuestiones regidas por la presente Convención y que ha sido debidamente facultada, de conformidad con sus procedimientos internos, para firmar, ratificar, aceptar o aprobar la Convención o adherirse a ella; las referencias a los “Estados partes” con arreglo a la presente Convención se aplicarán a esas organizaciones dentro de los límites de su competencia[12].

Por “proveedor de servicios” se entenderá: a) cualquier entidad pública o privada que proporcione a los usuarios de su servicio la posibilidad de comunicarse mediante

[6] Adaptado del 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, art. 2 c).
[7] Convención contra la Delincuencia Organizada, artículo 2 g).
[8] *Ibid.*, art. 2 f).
[9] *Ibid.*, art. 2 h).
[10] *Ibid.*, art. 2 e).
[11] *Ibid.*, art. 2 d).
[12] *Ibid.*, art. 2 j).

un sistema informático, y b) cualquier otra entidad que procese o almacene datos informáticos en nombre de dicho servicio de comunicación o de los usuarios de dicho servicio.

El término “conducta sexualmente explícita” incluye al menos los siguientes actos reales o simulados: a) relaciones sexuales, incluidas las genitales-genitales, las orales-genitales, las anales-genitales o las orales-anales, entre niños o entre un adulto y un niño; b) bestialidad; c) masturbación; d) abuso sádico o masoquista en un contexto sexual, o e) exhibición lasciva de los genitales o la zona púbica de un niño, ya sea vestido o desnudo.

Por “datos relativos al tráfico” se entenderá todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

Ámbito de aplicación

A menos que contenga una disposición en contrario, la presente Convención se aplicará a la prevención, la investigación y el enjuiciamiento de los delitos establecidos de conformidad con la Convención y la reunión, obtención y transmisión de pruebas electrónicas.

Protección de los derechos humanos y las libertades fundamentales y del estado de derecho

1. Los Estados partes cumplirán sus obligaciones en virtud de la presente Convención respetando plenamente los derechos humanos y las libertades fundamentales y el estado de derecho.

2. Nada de lo dispuesto en la presente Convención se interpretará en el sentido de que menoscaba otros derechos y obligaciones de los Estados y de las personas conforme al derecho internacional, en particular la Carta de las Naciones Unidas y el derecho internacional de los derechos humanos.

3. Toda persona que se encuentre detenida o respecto de la cual se adopte cualquier medida o sea encausada con arreglo a la presente Convención gozará de todos los derechos y garantías de conformidad con la legislación del Estado en cuyo territorio se encuentre y con las disposiciones pertinentes del derecho internacional de los derechos humanos, incluido el Pacto Internacional de Derechos Civiles y Políticos.

Protección de la soberanía[13]

1. Los Estados partes 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, jurisdicción o funciones que el derecho interno de ese Estado reserve exclusivamente a sus autoridades.

[13] Convención contra la Delincuencia Organizada y Convención contra la Corrupción, art. 4.

Venezuela (República Bolivariana de)

[Original: español]
[13 de abril de 2022]

4. Disposiciones generales

En este contexto, las disposiciones generales de la convención han de estar apegadas a los principios básicos del derecho internacional público y formar parte integral del futuro instrumento, consagrados estos en la Carta de las Naciones Unidas, lo que incluye, entre otros, el reconocimiento de la soberanía y la jurisdicción territorial conforme a la legislación nacional de los Estados, que abarca la aplicación del principio de soberanía al ciberespacio, la no injerencia en asuntos internos y respeto a la integridad territorial de los Estados y la solución pacífica de las controversias, entre otros.

Por su parte, la convención debe estipular el principio de complementariedad con otros instrumentos internacionales, tanto multilaterales como regionales, en lo que respecta al crimen transnacional, como la Convención de Naciones Unidas contra la Corrupción y la Convención de Naciones Unidas contra la Delincuencia Organizada Transnacional, entre otras, así como el respeto y cumplimiento de las responsabilidades en torno al derecho internacional de los derechos humanos, incluyendo las convenciones en materia de derechos humanos.

Al respecto, la República Bolivariana de Venezuela destaca que, tal y como ocurre con otros instrumentos jurídicos internacionales, no debe crearse en este instrumento una confrontación artificial entre los conceptos de soberanía nacional y derechos humanos, que son intrínsecamente complementarios.

En este capítulo, deberían incluirse definiciones de los términos y las expresiones fundamentales que se utilicen en la convención.

Viet Nam

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

Capítulo I. Disposiciones generales

1. Objetivos

a) Promover y fortalecer las medidas para prevenir y combatir más eficaz y eficientemente la utilización de las tecnologías de la información y las comunicaciones con fines delictivos;

b) Promover, facilitar y apoyar la cooperación internacional y la asistencia técnica en la prevención y la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos, incluida la recuperación de activos, de conformidad con los principios fundamentales del derecho internacional y de manera respetuosa de los derechos humanos.

2. Ámbito de aplicación

La presente Convención se aplicará a la prevención, investigación y enjuiciamiento del uso de las tecnologías de la información y las comunicaciones con fines delictivos.

3. Protección de la soberanía

a) Los Estados Miembros cumplirán sus obligaciones con arreglo a la presente Convención en consonancia con los principios de igualdad soberana, integridad territorial de los Estados y no amenaza ni uso de la fuerza, así como de no intervención en los asuntos internos de otros Estados;

b) Nada de lo dispuesto en la presente Convención facultará a un Estado Miembro para ejercer, en el territorio de otro Estado, jurisdicción o funciones que el derecho interno de ese Estado Miembro reserve exclusivamente a sus autoridades.

4. Definiciones

a) Por “ciberespacio” se entenderá una red de infraestructuras de tecnologías de la información que incluye redes de telecomunicaciones, Internet, redes de computadoras, sistemas de comunicación, sistemas de procesamiento y control de la información y bases de datos;

b) Por “sistema de información” se entenderá una combinación de *hardware*, *software* y bases de datos establecida para servir a la creación, transmisión, recogida, procesamiento y almacenamiento de información en el ciberespacio;

c) Por “ciberataque” se entenderá la utilización del ciberespacio, la tecnología de la información o los dispositivos electrónicos para sabotear o interrumpir la red de telecomunicaciones, Internet, la red de computadoras, los sistemas de comunicación, los sistemas de procesamiento y control de la información, las bases de datos o los dispositivos electrónicos;

d) Por “ciberterrorismo” se entenderá un acto de terrorismo o de financiación del terrorismo que implique el uso del ciberespacio, de las tecnologías de la información o de dispositivos electrónicos;

e) Por “información personal” se entenderá la información asociada a la identificación de una persona física;

f) Los datos digitales están compuestos por señales, letras, números, imágenes, sonidos o elementos similares creados, almacenados y transmitidos o adquiridos por medios electrónicos;

g) Por “infraestructura cibernética” se entenderá un sistema de infraestructura que sirve para la creación, la transmisión, la recogida, el procesamiento y el almacenamiento de información y datos en el ciberespacio.