Naciones Unidas A/AC.291/9

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

Resumen

Como parte de los preparativos del segundo período de sesiones del Comité Especial encargado de Elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos, la Presidenta del Comité elaboró con el apoyo de la secretaría el presente documento, que contiene propuestas recibidas de los Estados Miembros sobre las disposiciones relativas a la criminalización (A/AC.291/9), las disposiciones generales (A/AC.291/9/Add.1) y las disposiciones sobre las medidas procesales y la aplicación de la ley (A/AC.291/9/Add.2).

V.22-02326 (S) 190522 190522

Se ruega reciclar

Índice

		Página
I.	Introducción	3
II.	Criminalización	3
	Angola	3
	Australia	4
	Brasil	7
	Burundi	11
	Canadá	14
	Colombia	17
	Egipto	18
	El Salvador	23
	Unión Europea y sus Estados miembros	27
	Ghana	29
	Irán (República Islámica del)	35
	Japón	35
	Jordania	38
	México	40
	Nueva Zelandia	41
	Noruega	45
	Federación de Rusia, también en nombre de Belarús, Burundi, China, Nicaragua y Tayikistán	46
	Sudáfrica	52
	Suiza	56
	Reino Unido de Gran Bretaña e Irlanda del Norte	59
	República Unida de Tanzanía	64
	Estados Unidos de América	65
	Venezuela (República Bolivariana de)	70
	Viet Nam	72

I. Introducción

1. Como parte de los preparativos del segundo período de sesiones del Comité Especial encargado de Elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos, y en consonancia con la hoja de ruta y el modo de trabajo del Comité Especial aprobados en su primer período de sesiones, en particular sus párrafos 3 y 4, se invitó a los Estados Miembros a que proporcionaran a la secretaría versiones preliminares del texto de los capítulos o las disposiciones que se examinarían durante el segundo período de sesiones, respecto de las disposiciones sobre criminalización (A/AC.291/9), las disposiciones generales (A/AC.291/9/Add.1) y las disposiciones sobre las medidas procesales y la aplicación de la ley (A/AC.291/9/Add.2).

2. Sobre esa base, la Presidenta del Comité, con el apoyo de la secretaría, preparó el presente documento de negociación que contiene una recopilación de las propuestas y las contribuciones de los Estados Miembros, centradas en los capítulos específicos que se examinarán durante el segundo período de sesiones. Así pues, el presente documento contiene únicamente sugerencias de redacción específicas u observaciones generales sobre los capítulos relativos a la criminalización, las disposiciones generales y las medidas procesales y la aplicación de la ley, agrupadas por capítulos, tal como se recibieron de los Estados Miembros y traducidas a los seis idiomas oficiales de las Naciones Unidas. Salvo que se indique otra cosa, las notas de pie de página contienen el texto tal como se recibió de los Estados Miembros.

3. Como se ha mencionado con anterioridad, el presente documento no contiene observaciones sobre otros temas ni explicaciones de las distintas sugerencias de redacción, que pueden encontrarse en las comunicaciones originales, publicadas en el sitio web del Comité Especial tal como se recibieron y en su versión original en el momento de su recepción.

4. A fecha 14 de abril de 2022, la secretaría había recibido 24 comunicaciones, que representaban la opinión de 54 Estados Miembros y de la Unión Europea.

II. Criminalización

Angola

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

- La convención debería tipificar como delito y criminalizar las conductas de ciberdelincuencia más graves, especialmente cuando afectaran a infraestructuras críticas, clasificándolas como ciberterrorismo o crímenes de lesa humanidad, y definir normas prioritarias y urgentes en materia de cooperación internacional para la investigación y enjuiciamiento de los agentes de la ciberdelincuencia.
- La convención debería tipificar como delito y criminalizar las conductas de ciberdelincuencia en que se utilizaran criptomonedas y criptoactivos para financiar el terrorismo y blanquear dinero.

Criminalización

Delitos basados en la cibernética (delitos contra la confidencialidad, la integridad y la disponibilidad de los sistemas y los datos informáticos): acceso ilícito, interceptación ilícita, daños a datos informáticos, sabotaje informático, falsedad informática y reproducción ilícita de un programa informático.

Delitos que se valen de la cibernética como instrumento (delitos tradicionales cometidos utilizando las tecnologías de la información y las comunicaciones): estafas en línea, suplantación de identidad (*phishing*), delitos económicos y financieros en

línea, usurpación de identidad en línea, abusos y explotación sexuales de niños en línea, ciberacoso, ciberhostigamiento, pornovenganza y ciberterrorismo.

Para la definición de estos tipos penales, se puede acudir a los instrumentos jurídicos regionales e internacionales mencionados anteriormente[1].

Australia

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

Criminalización

La nueva convención brinda la oportunidad de mejorar la cooperación internacional en materia de ciberdelincuencia, asegura la coherencia entre los tratados internacionales relativos a la delincuencia y otros instrumentos pertinentes vigentes y evita la duplicación innecesaria entre estos. Los artículos relativos a la criminalización deberían ser compatibles con los instrumentos internacionales vigentes y evitar conflictos entre esos instrumentos. Los artículos relativos a la criminalización también deberían mantener un equilibrio adecuado con el estado de derecho, los derechos humanos y las libertades fundamentales.

Australia considera que la nueva convención brinda la oportunidad de lograr una mayor armonización mundial de los delitos de ciberdelincuencia, lo cual, a su vez, reducirá los refugios seguros para los ciberdelincuentes y aumentará la capacidad de las fuerzas del orden para combatir la actividad de la ciberdelincuencia en línea.

Las disposiciones de derecho penal sustantivo de la nueva convención deberían ser específicas y articular claramente la conducta penal subyacente. En la convención también se debería prestar la debida atención a los delitos determinantes y a las otras formas de responsabilidad por los delitos basados en la cibernética o facilitados por esta. Ello debería incluir la habitual extensión de la responsabilidad penal prevista en instrumentos como la Convención de las Naciones Unidas contra la Delincuencia Organizada y la Convención de las Naciones Unidas contra la Corrupción.

Delitos basados en la cibernética

Australia considera que la nueva convención debería incluir normas sobre la criminalización de delitos dirigidos a sistemas informáticos (“delitos basados en la cibernética”). Australia propone la inclusión de los siguientes delitos basados en la cibernética en la nueva convención:

- el acceso ilícito e ilegítimo a cualquier parte de un sistema informático (incluidos datos informáticos);
- la interceptación ilícita e ilegítima de datos informáticos en transmisiones;
- el ataque ilícito e ilegítimo a la integridad de datos informáticos (incluidos el borrado, el deterioro, la alteración o la supresión de datos informáticos);
- la interferencia ilícita en el funcionamiento de un sistema o red informática;
- la producción, el suministro, la distribución o la obtención de programas informáticos maliciosos con el fin de cometer otro delito cibernético.

[1] Nota de la secretaría: se hace referencia a los instrumentos mencionados en la sección relativa al preámbulo de la comunicación de Angola, a saber, la Convención de la Unión Africana sobre la Ciberseguridad y la Protección de los Datos Personales (Convención de Malabo), el Convenio del Consejo de Europa sobre la Ciberdelincuencia (Convenio de Budapest), la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y la Convención de las Naciones Unidas contra la Corrupción.

Delitos facilitados por la cibernética

El derecho penal vigente en casi todos los Estados resulta suficiente para definir delitos conocidos como la violación de domicilio, el vandalismo, el robo, los delitos relacionados con estupefacientes y otros delitos violentos.

No es necesario que la convención vuelva a definir esos delitos tan solo porque en su comisión entre en juego un sistema informático o la tecnología digital si la utilización de un sistema informático en la comisión del delito no cambia la configuración o la gravedad de la conducta delictiva.

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

Si bien Australia cree que en la convención se debería aplicar un enfoque restrictivo en lo que respecta a crear cualquier categoría de delito nueva, está abierta a argumentos en favor de que la convención no solo incluya los delitos basados en la cibernética, sino que se amplíe a los delitos facilitados por la cibernética.

Con tal fin, Australia observó con aprecio los numerosos llamamientos a hacer frente a la grave amenaza que supone la explotación y los abusos sexuales de niños en línea que se hicieron durante el primer período de sesiones del Comité Especial. En opinión de Australia, se trata de una cuestión respecto de la cual los países pueden trabajar de manera constructiva para llegar a un consenso. Reconociendo la gravedad de estos delitos, Australia ha formulado una propuesta aparte para los delitos de abusos de niños en línea, que incluyen la captación de niños por Internet con fines sexuales y la emisión en directo de los abusos.

Australia también considera que el aumento notable del fraude y el robo facilitados por la cibernética, incluida la extorsión vinculada a programas secuestradores, es una cuestión generalizada respecto de la cual los Estados pueden llegar a un consenso para criminalizar esta conducta a los efectos de la convención.

Criminalización de los delitos de abusos de niños en línea

Artículo [A]: Material que muestre abusos de niños mediante un sistema informático

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada [sin motivo lícito][2] de los siguientes actos:

a) acceder a material que muestre abusos de niños, controlar, transmitir, distribuir, ofrecer, obtener, producir o poner a disposición ese material a través de un sistema informático[3], o

[2] Esta salvedad se incluye para que el delito no abarque involuntariamente determinadas situaciones legítimas: por ejemplo, aquellos supuestos en que podría haber la necesidad médica de acceder al material o de producirlo y que de otra manera quedarían comprendidos en esta disposición.

[3] Por "sistema informático" se entiende 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. Esto puede incluir dispositivos de entrada, salida y almacenamiento. También incluiría sistemas autónomos o sistemas en red con otros dispositivos. Nótese que este término (o su definición) podría ser objeto de modificaciones en aras de la coherencia con otras disposiciones del proyecto de convención.

b) poseer material que muestre abusos de niños fruto de los actos enunciados en el párrafo 1 a).

2. A los efectos del artículo [A], el término “material que muestre abusos de niños” incluirá todo material que represente o describa a un niño, o la representación de un niño, que implícitamente esté, o parezca estar, realizando actividades sexuales o en presencia de una persona que realice actividades sexuales, así como toda representación de las partes genitales de un niño[4] con fines primordialmente sexuales, o que sea, o parezca ser, víctima de la tortura o tratos o penas crueles, inhumanos o degradantes.

Artículo [B]: Facilitación de material que muestra abusos de niños mediante un sistema informático

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado [sin motivo lícito][5] que cree, desarrolle, altere, mantenga, controle, modere, asista[6], ponga a disposición, publicite o promueva un sistema informático con el fin de facilitar material que muestre abusos de niños en los términos expuestos en el artículo [A].

2. A los efectos del párrafo 1, por la expresión “facilitar material que muestre abusos de niños” se entenderá cualquiera de los actos enumerados en el párrafo 1 que se realicen para que las personas puedan acceder a “material que muestre abusos de niños” y transmitir, distribuir, ofrecer, poner a disposición o producir ese material para sí mismas u otras personas.

Artículo [C]: Captación u obtención de niños con fines sexuales mediante un sistema informático

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada mediante un [sistema informático] de actos consistentes en captar niños con fines sexuales, hacerles una proposición, obtenerlos o hacer que protagonicen encuentros, sean testigos de actividades sexuales o participen en ellas.

Artículo [X]: Disposiciones generales relativas a la propuesta

1. A los efectos de los artículos [A, B, C], se entenderá por “niño” toda persona menor de 18 años. Además, a los efectos del artículo [C], la palabra “niño” también incluye a una persona que se crea es menor de 18 años[7]. A los efectos de los artículos [A, B, C], los Estados partes podrán, no obstante, exigir un límite de edad inferior, que deberá ser como mínimo de 16 años.

2. A los efectos de los artículos [A, B, C], tendrán responsabilidad penal las personas de 18 años o más. Los Estados partes podrán declarar en cualquier momento que las personas menores de 18 años tendrán responsabilidad penal. Si un Estado parte formula esa declaración, velará por que haya las salvaguardias apropiadas en su ordenamiento jurídico para proteger al niño acusado, teniendo presentes los efectos que un proceso judicial penal puede tener para un niño.

El material autogenerado puede comprender tanto el material puramente autogenerado como el material autogenerado bajo coacción o extorsión. En esos contextos, la disposición pretende fijar una postura general de prudencia adicional en torno a la criminalización al tiempo que deja margen a los ordenamientos jurídicos internos para que decidan su respuesta proporcionada y razonable.

[4] Terminología procedente 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.

[5] Al igual que la nota 2.

[6] Se podría acabar incluyendo el contenido de la palabra “asistir” si se amplían las disposiciones generales relativas a la responsabilidad penal. Se mantiene aquí hasta que se examinen esas disposiciones.

[7] Esta adición de la creencia tiene por objeto abarcar las situaciones en que una persona de interés o una persona que esté siendo investigada por captación u obtención de niños con fines sexuales interactúe en línea con un funcionario encargado de hacer cumplir la ley que opere encubierto.

3. En el caso de que un Estado parte trate de penalizar a las personas menores de 18 años por algún supuesto previsto en el artículo [A], tendrá debidamente en cuenta la necesidad de evitar la penalización excesiva de los niños que hayan autogenerado material comprendido en el artículo [A], párrafo 2, así como la necesidad de respetar las obligaciones que le incumben en virtud de la Convención sobre los Derechos del Niño y sus Protocolos.

Penas asociadas

Proponemos la inclusión de un artículo en que se establezca la obligación de los Estados partes de adoptar las medidas legislativas y de otra índole que resulten necesarias para que todo delito tipificado con arreglo a la presente convención esté sujeto a sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad.

Brasil

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

Capítulo II
Criminalización

Artículo 4
Acceso ilícito[8]

Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a todo o parte de un sistema informático. Las Partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático.

Artículo 5
Ataques a la integridad de los datos[9]

Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos. Las Partes podrán reservarse el derecho a exigir que los actos descritos en el párrafo comporten daños graves.

Artículo 6
Ataques a la integridad del sistema[10]

Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

Artículo 7
Interceptación ilícita[11]

Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos en transmisiones no públicas

[8] *Fuente*: Convenio del Consejo de Europa sobre la Ciberdelincuencia (Convenio de Budapest).
[9] *Fuente*: Convenio del Consejo de Europa sobre la Ciberdelincuencia.
[10] *Fuente*: Convenio del Consejo de Europa sobre la Ciberdelincuencia.
[11] *Fuente*: Convenio del Consejo de Europa sobre la Ciberdelincuencia.

dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro de este, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos. Las Partes podrán exigir que el delito se cometa con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

Artículo 8
Fraude informático[12]

Las Partes adoptarán las medidas legislativas o de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante:

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

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

con la intención fraudulenta o delictiva de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.

Artículo 9
Acceso ilícito a contraseñas y credenciales[13]

Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado e ilegítimo por el que se consigan, obtengan o reciban contraseñas o credenciales de acceso a un sistema informático.

Artículo 10
Uso indebido de los dispositivos[14]

1. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a) la producción, venta, obtención para su utilización, importación, distribución o cualquier otra forma de puesta a disposición de:

i) cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos tipificados con arreglo a los artículos 4 a 9;

ii) una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático;

con intención de que sean utilizados para cometer cualquiera de los delitos tipificados con arreglo a los artículos 4 a 9, y

b) la posesión de alguno de los elementos contemplados en los incisos i) o ii) del apartado a) del presente párrafo, con intención de que sean utilizados para cometer cualquiera de los delitos tipificados con arreglo a los artículos 4 a 9. Las Partes podrán exigir en su derecho interno la posesión de un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

2. No se interpretará que el presente artículo impone responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, distribución o cualquier otra forma de puesta a disposición o la posesión mencionada en el párrafo 1 del presente artículo no tenga por objeto la comisión de uno de los delitos tipificados con arreglo a los artículos 4 a 9 de la presente Convención, como en el caso de las pruebas autorizadas o de la protección de un sistema informático.

[12] *Fuente*: Convenio del Consejo de Europa sobre la Ciberdelincuencia.
[13] *Fuente*: propuesta original del Brasil.
[14] *Fuente*: Convenio del Consejo de Europa sobre la Ciberdelincuencia.

3. Las Partes podrán reservarse el derecho a no aplicar el párrafo 1 del presente artículo, siempre que dicha reserva no afecte a la venta, distribución o cualquier otra forma de puesta a disposición de los elementos mencionados en el inciso ii) del párrafo 1 a) del presente artículo.

Artículo 11
Falsificación informática[15]

Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente. Las Partes podrán exigir que exista una intención fraudulenta o delictiva similar para que se considere que existe responsabilidad penal.

Artículo 12
Delitos relacionados con la pornografía infantil[16]

1. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a) la producción de pornografía infantil con la intención de distribuirla a través de un sistema informático;

b) la oferta o la puesta a disposición de pornografía infantil a través de un sistema informático;

c) la distribución o la transmisión de pornografía infantil a través de un sistema informático;

d) la obtención, para uno mismo o para otra persona, de pornografía infantil a través de un sistema informático;

e) la posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos.

2. A los efectos del párrafo 1 anterior, se entenderá por “pornografía infantil” todo material pornográfico que contenga la representación visual de:

a) un menor adoptando un comportamiento sexualmente explícito;

b) una persona que parezca un menor adoptando un comportamiento sexualmente explícito;

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

3. A los efectos del párrafo 2 anterior, se entenderá por “menor” toda persona menor de 18 años. Las Partes podrán, no obstante, exigir un límite de edad inferior, que deberá ser como mínimo de 16 años.

4. Las Partes podrán reservarse el derecho a no aplicar, en todo o en parte, los apartados d) y e) del párrafo 1 y los apartados b) y c) del párrafo 2.

Artículo 13
Incitación o coacción para cometer suicidio[17]

Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la incitación o la coacción,

[15] *Fuente*: Convenio del Consejo de Europa sobre la Ciberdelincuencia.
[16] *Fuente*: Convenio del Consejo de Europa sobre la Ciberdelincuencia.
[17] *Fuente*: Propuesta de China y la Federación de Rusia.

también de menores, para cometer suicidio mediante presión psicológica o de otra índole en las redes de información y telecomunicaciones, inclusive Internet.

Artículo 14
Infracción de los derechos de autor y derechos afines por medio de las tecnologías de la información y las comunicaciones[18]

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito o reconocer como acto ilícito en su derecho interno las infracciones de los derechos de autor y de los derechos afines, tal y como se definen en la legislación de ese Estado parte, cuando esos actos sean cometidos deliberadamente por medio de las tecnologías de la información y las comunicaciones, incluidos el uso ilícito de programas informáticos para sistemas informáticos o bases de datos protegidos por derechos de autor y la apropiación de la autoría.

Artículo 15
Tentativa y complicidad[19]

1. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno cualquier complicidad deliberada con vistas a la comisión de alguno de los delitos tipificados con arreglo al capítulo II de la Convención.

2. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno toda tentativa deliberada de cometer alguno de los delitos tipificados con arreglo al capítulo II de la Convención.

3. Las Partes podrán reservarse el derecho a no aplicar, en todo o en parte, el párrafo 2 del presente artículo.

Artículo 16
Responsabilidad de las personas jurídicas[20]

1. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para que pueda exigirse responsabilidad a una persona jurídica por los delitos tipificados con arreglo a la presente Convención, cuando sean cometidos por cuenta de esta por una persona física, ya sea a título individual o como miembro de un órgano de dicha persona jurídica, que ejerza funciones directivas en su seno, en virtud de:

a) un poder de representación de la persona jurídica;

b) una autorización para tomar decisiones en nombre de la persona jurídica;

c) una autorización para ejercer funciones de control en el seno de la persona jurídica.

2. Además de los casos previstos en el párrafo 1 del presente artículo, cada Parte adoptará las medidas necesarias para garantizar que pueda exigirse responsabilidad a una persona jurídica cuando la ausencia de vigilancia o de control por parte de cualquier persona física mencionada en el párrafo 1 haya permitido la comisión de un delito tipificado con arreglo a la presente Convención por una persona física que actúe por cuenta de dicha persona jurídica y bajo su autoridad.

3. Dependiendo de los principios jurídicos de cada Parte, la responsabilidad de una persona jurídica podrá ser penal, civil o administrativa.

4. Dicha responsabilidad se entenderá sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido el delito.

[18] *Fuente*: Propuesta de China y la Federación de Rusia.
[19] *Fuente*: Convenio del Consejo de Europa sobre la Ciberdelincuencia, con cambios introducidos por el Brasil.
[20] *Fuente*: Convenio del Consejo de Europa sobre la Ciberdelincuencia.

Artículo 17
Sanciones y medida[21]

1. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para que los delitos tipificados con arreglo al capítulo II de la Convención estén sujetos a sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad.

2. Las Partes garantizarán la imposición de sanciones o medidas penales o no penales efectivas, proporcionadas y disuasorias, incluidas sanciones pecuniarias, a las personas jurídicas consideradas responsables de conformidad con el artículo 16.

Burundi

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

Capítulo II. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos

Sección 1
Ataques a la confidencialidad de los sistemas informáticos

Sección 2
Acceso ilícito

Los Estados partes en la presente Convención tipificarán como delito en su derecho interno el acceso deliberado e ilegítimo a todo o parte de un sistema informático.

Sección 3
Ataques a la integridad de un sistema informático

Los Estados partes en la presente Convención tipificarán como delito en su derecho interno todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos.

Sección 4
Ataques a la integridad de los datos

Los Estados partes en la presente Convención tipificarán como delito, sin perjuicio de su derecho interno, la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

Sección 5
Fabricación, venta, compra, utilización, importación, distribución o posesión ilícita de un sistema informático e incitación al suicidio

Los Estados partes en la presente Convención tipificarán como delito, sin perjuicio de su derecho interno, la fabricación, venta, compra, utilización, importación, distribución o posesión de una computadora o un sistema informático o la puesta a disposición de datos, programas o sistemas informáticos con la intención de utilizarlos o ponerlos a disposición de otras personas con el fin de cometer algún delito.

Sección 6
Fraude informático

Los Estados partes en la presente Convención tipificarán como delito, sin perjuicio de su derecho interno, los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante: a) la introducción, alteración, borrado o supresión

[21] *Fuente*: Convenio del Consejo de Europa sobre la Ciberdelincuencia.

de datos informáticos o b) cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.

§1. Estafa en los sistemas informáticos

Los Estados partes en la presente Convención tipificarán como delito, sin perjuicio de su derecho interno, la manipulación fraudulenta, por medio de la comunicación electrónica, para obtener o tratar de obtener dinero, bienes muebles, bonos, depósitos, instrumentos, cauciones, recibos, quitas o la totalidad o una parte del patrimonio de otra persona.

§2. Usurpación de la identidad digital

Los Estados partes en la presente Convención tipificarán como delito, sin perjuicio de su derecho interno, el hecho de asumir la identidad digital de otra persona o la utilización de uno o más datos de cualquier naturaleza que identifique a esa persona con el fin de perturbar su tranquilidad o atentar contra su reputación, su vida privada, su patrimonio, o el de terceros, para lucrarse o inducir a error a otras personas.

§3. Suplantación de identidad (*phishing*)

Los Estados partes en la presente Convención tipificarán como delito, sin perjuicio de su derecho interno, la utilización de un sitio web o el envío de un mensaje electrónico con la ayuda de un sistema informático con la intención de obtener información confidencial de la persona que visite el sitio web o del destinatario del mensaje para utilizar esa información con fines delictivos.

§4. Abuso de confianza en relación con datos informáticos

Los Estados partes en la presente Convención tipificarán como delito, sin perjuicio de su derecho interno, la apropiación indebida o la distracción de datos informáticos confiados a una persona en virtud de un título que produzca la obligación de restituirlos o hacer un uso determinado de ellos.

§5. Receptación ilícita de datos informáticos

Los Estados partes en la presente Convención tipificarán como delito, sin perjuicio de su derecho interno, la posesión, por cualquier título, de datos informáticos a sabiendas de que se han obtenido mediante la comisión de un delito.

§ 6. Extorsión de datos informáticos

Los Estados partes en la presente Convención tipificarán como delito, sin perjuicio de su derecho interno, la tentativa de obtener datos informáticos valiéndose de la fuerza, la violencia o la coacción.

§7. Chantaje y publicación de rumores

Los Estados partes en la presente Convención tipificarán como delito, sin perjuicio de su derecho interno, el hecho de amenazar por escrito o de palabra, revelar o imputar hechos difamatorios o conseguir o tratar de conseguir datos informáticos mediante la extorsión.

§ 8. Envío de mensajes no solicitados (*spamming*)

Los Estados partes en la presente Convención tipificarán como delito, sin perjuicio de su derecho interno, los siguientes actos:

1. el envío de mensajes no solicitados de manera reiterada o a un gran número de personas utilizando una computadora o un sistema informático;

2. la utilización de una computadora o un sistema informático para reenviar un mensaje recibido a múltiples personas o reenviarlo múltiples veces a una persona que no lo necesite.

Sección 7
Delitos relacionados con el contenido

§1. Delitos relacionados con la pornografía infantil

Los Estados partes en la presente Convención tipificarán como delito, sin perjuicio de su derecho interno, los siguientes actos cuando sean cometidos deliberada e ilegítimamente: la producción de pornografía infantil con la finalidad de distribuirla a través de un sistema informático y la oferta o la puesta a disposición de pornografía infantil a través de un sistema.

Sección 8
Escritos e imágenes de carácter racista o xenófobo a través de un sistema informático

Los Estados partes en la presente Convención tipificarán como delito, sin perjuicio de su derecho interno, la creación, descarga, diseminación o puesta a disposición en cualquier formato de escritos, mensajes, fotografías, dibujos, videos o cualquier otra representación de ideas o teorías de carácter racista o xenófobo por medio de un sistema informático.

Sección 9
Injuria cometida por medio de un sistema informático

Los Estados partes en la presente Convención tipificarán como delito, sin perjuicio de su derecho interno, las injurias dirigidas a una persona por su pertenencia a un grupo caracterizado por la raza, el color, la ascendencia, el origen nacional o étnico o la religión, en la medida en que se utilice como pretexto para cualquiera de esos factores, o a un grupo de persona que se distinga por cualquiera de esas características.

Sección 10
Delitos relacionados con el terrorismo, la fabricación de armas, la trata de personas o el tráfico de estupefacientes cometidos con la ayuda de una computadora o un sistema informático

§1. Creación o publicación de un sitio para grupos terroristas

Los Estados partes en la presente Convención tipificarán como delito, sin perjuicio de su derecho interno, los siguientes actos:

1. el establecimiento, la publicación o la utilización del sitio web de un grupo terrorista con la ayuda de Internet, una computadora o un sistema informático con el fin de facilitar la comunicación a sus líderes o sus miembros;

2. la movilización de fondos o la diseminación de sus ideas o conocimientos sobre el modo en que lleva a cabo sus operaciones terroristas.

§2. Diseminación de los métodos o medios de destrucción

Los Estados partes en la presente Convención tipificarán como delito, sin perjuicio de su derecho interno, todo acto por el que se disemine o se ponga a disposición de otras personas a través de un sistema informático, salvo que tenga como destinatario a personas autorizadas, manuales de instrucciones o métodos de fabricación de armas de fuego, sus piezas, componentes y municiones de naturaleza tal que atenten contra la vida humana, los bienes o el medio ambiente.

§3. Creación o publicación de un sitio con fines de trata de personas

Los Estados partes en la presente Convención tipificarán como delito, sin perjuicio de su derecho interno, el establecimiento o la publicación de un sitio en una red de

información, un equipo informático o un sistema informático con fines de trata de personas o de facilitar esa transacción.

§4. Creación o publicación de un sitio con fines de tráfico o distribución de drogas o estupefacientes

Los Estados partes en la presente Convención tipificarán como delito, sin perjuicio de su derecho interno, la creación o la publicación de un sitio en una red de información, un equipo informático o un sistema informático con fines de tráfico o distribución de drogas o estupefacientes o de facilitar esa transacción.

Sección 11
Asociación delictiva relacionada la cibernética

Los Estados partes en la presente Convención tipificarán como delito, sin perjuicio de su derecho interno, la participación deliberada en una asociación constituida o una conspiración establecida con el fin de preparar o cometer uno o más delitos.

Sección 12
Delitos relacionados con infracciones de la propiedad intelectual y los derechos afines

Los Estados partes en la presente Convención tipificarán como delito, sin perjuicio de su derecho interno, las infracciones de la propiedad intelectual.

Capítulo III. Responsabilidad de las personas jurídicas

Los Estados partes en la presente Convención adoptarán las disposiciones que resulten necesarias para que pueda exigirse responsabilidad a las personas jurídicas por los delitos tipificados con arreglo a la presente Convención.

Adoptarán las medidas necesarias para garantizar que pueda exigirse responsabilidad a una persona jurídica por falta de vigilancia o control por parte de cualquier persona física que trabaje en su seno. La responsabilidad de una persona jurídica podrá ser penal, civil o administrativa.

Canadá

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

Delitos

Acceso ilícito a un sistema informático

Tipificar como delito el acceso fraudulento e ilegítimo a todo o parte de un sistema informático.

Interceptación ilícita de sistemas informáticos en transmisiones no públicas

Tipificar como delito la interceptación fraudulenta e ilegítima, por cualquier medio técnico, de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro de este, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos.

Ataques a la integridad de los datos informáticos

Tipificar como delito todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos.

Ataques a la integridad del sistema informático

Tipificar como delito la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

Uso indebido de los dispositivos

1. Tipificar como delito la comisión deliberada e ilegítima de los siguientes actos:

a) la producción, venta, obtención para su utilización, importación, distribución o cualquier otra forma de puesta a disposición de:

i) cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos cibernéticos previstos en la presente Convención;

ii) una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con intención de que sean utilizados para cometer cualquiera de los delitos cibernéticos previstos en la Convención, y

b) la posesión de alguno de los elementos contemplados en los incisos i) o ii) del apartado a) del presente párrafo, con intención de que sean utilizados para cometer cualquiera de los delitos cibernéticos previstos en la presente Convención.

2. No se interpretará que el presente artículo impone responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, distribución o cualquier otra forma de puesta a disposición o la posesión mencionada en el párrafo 1 no tenga por objeto la comisión de uno de los delitos cibernéticos previstos en la presente Convención, como en el caso de las pruebas autorizadas o de la protección de un sistema informático.

Delitos relacionados con la explotación sexual de niños

1. Tipificar como delito la comisión deliberada e ilegítima de los siguientes actos:

a) la producción de material que muestre explotación sexual de niños con la intención de distribuirlo a través de un sistema informático;

b) la oferta, publicidad o puesta a disposición de material que muestre explotación sexual de niños a través de un sistema informático;

c) la distribución o transmisión de material que muestre explotación sexual de niños a través de un sistema informático;

d) la obtención, para uno mismo o para otra persona, de material que muestre explotación sexual de niños a través de un sistema informático;

e) el acceso a material que muestre explotación sexual de niños o su posesión en un sistema informático o en un dispositivo de almacenamiento de datos informáticos.

2. A los efectos del párrafo 1, se entenderá por “material que muestre explotación sexual de niños” la pornografía infantil según se define en el Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía, así como todo:

a) material visual, incluidos medios fotográficos, en video y de emisión en directo, que contenga la representación de:

i) un niño realizando actividades sexuales o estando en presencia de ellas;

ii) una persona que parezca ser un niño realizando actividades sexuales o estando en presencia de ellas;

iii) imágenes realistas que representen a un niño realizando actividades sexuales o estando en presencia de ellas;

b) material escrito que:

i) defienda las actividades sexuales con un niño;

ii) esté escrito con fines sexuales y cuya característica dominante sea la descripción de actividades sexuales con un niño, y

c) grabaciones de audio que:

i) defiendan las actividades sexuales con un niño;

ii) estén realizadas con fines sexuales y cuya característica dominante sea la descripción de actividades sexuales con un niño.

Captación y tentación de niños con fines sexuales

1. Tipificar como delito la comisión deliberada e ilegítima de los siguientes actos:

a) transmitir, distribuir, vender o poner a disposición mediante un sistema informático material sexualmente explícito a un niño o a una persona que se crea que es un niño;

b) comunicarse con un niño, o una persona que se crea es un niño, mediante un sistema informático, o

c) acordar o concertar arreglos con un niño, o una persona que se crea es un niño, mediante un sistema informático;

a los efectos de facilitar la comisión de cualquiera de los delitos relacionados con la explotación sexual de niños tipificados con arreglo a la presente Convención, el Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía o el derecho interno del Estado parte.

2. No se exigirá responsabilidad penal si una persona ha adoptado medidas razonables para verificar que la persona en cuestión no es un niño.

Diseminación no consentida de imágenes íntimas (“pornovenganza”)

1. Tipificar como delito la publicación, distribución, transmisión, venta, puesta a disposición o publicidad deliberada e ilegítima de una imagen íntima de una persona por medio de un sistema informático, a sabiendas de que la persona representada en la imagen no prestó su consentimiento a dicho acto o con temeridad respecto al consentimiento prestado por esa persona a dicho acto.

2. A los efectos del párrafo 1, por “imagen íntima” se entenderá toda grabación visual de una persona realizada por cualquier medio, incluida la grabación fotográfica, filmográfica o en video:

a) en la cual la persona esté desnuda, exponga los genitales, la región anal o los pechos o realice actividades sexuales explícitas;

b) respecto de la cual, en el momento de llevarse a cabo, hubiera circunstancias que dieran lugar a una expectativa razonable de privacidad, y

c) respecto de la cual la persona representada tenga una expectativa razonable de privacidad en el momento de la comisión del delito.

3. No se exigirá responsabilidad penal si la difusión no consentida persigue el bien público o una finalidad legítima.

Colombia

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

3. Criminalización

En cuanto a los delitos basados en la cibernética, cada Estado Miembro debería adoptar las medidas legislativas y de otra índole necesarias para tipificar como delito, en su ordenamiento jurídico interno, las siguientes conductas:

a) Acceso ilícito: Acceder ilegítimamente a todo o parte de un sistema informático[22].

b) Interceptación ilícita: Interceptar ilegítimamente datos informáticos, tanto en su origen, destino o en el interior de un sistema informático, como en las emisiones electromagnéticas provenientes de un sistema informático que los transporta[23].

c) Ataques a la integridad de los datos: Dañar, destruir, borrar, deteriorar, alterar o suprimir datos informáticos o un sistema de tratamiento de información o sus partes o componentes lógicos[24].

d) Ataques a la integridad del sistema: Obstaculizar ilegítimamente el funcionamiento o el acceso normal a un sistema informático, a los datos allí contenidos o a una red de telecomunicaciones[25].

e) Abuso de los dispositivos: Producir, obtener, poseer, comerciar o difundir un dispositivo, incluido un programa informático, así como una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático, para la comisión de los delitos señalados en los literales a), b), c) y d) del presente acápite[26].

f) Falsificación informática: Introducir, alterar, borrar o suprimir deliberada e ilegítimamente datos informáticos de modo que se generen datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos[27].

En cuanto a los delitos facilitados por la cibernética, cada Estado Miembro debería adoptar las medidas legislativas y de otra índole necesarias para tipificar como delito, en su ordenamiento jurídico interno, las siguientes conductas:

a) Delitos relacionados con material de abuso sexual infantil: Producir, ofertar, difundir, transmitir, adquirir o poseer, a través de un sistema informático, material de abuso sexual infantil[28].

b) Fraude informático: Introducir, alterar, borrar, suprimir datos informáticos, o interferir en el funcionamiento de un sistema informático, con la intención dolosa o culposa de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona, en perjuicio del patrimonio de otra persona[29].

c) Violación de datos personales: Obtener, compilar, sustraer, ofrecer, vender, intercambiar, enviar, comprar, interceptar, divulgar, modificar o emplear, sin estar

[22] Artículo 2 del Convenio de Budapest sobre la Ciberdelincuencia. En consonancia con el artículo 269A de la Ley 1273 de 2009.
[23] Artículo 3 del Convenio de Budapest sobre la Ciberdelincuencia. En consonancia con el artículo 269C de la Ley 1273 de 2009.
[24] Artículo 4 del Convenio de Budapest sobre la Ciberdelincuencia. En consonancia con el artículo 269D de la Ley 1273 de 2009.
[25] Artículo 5 del Convenio de Budapest sobre la Ciberdelincuencia. En consonancia con el artículo 269B de la Ley 1273 de 2009.
[26] Artículo 6 del Convenio de Budapest sobre la Ciberdelincuencia.
[27] Artículo 7, ibídem.
[28] Artículo 9, ibídem.
[29] Artículo 8, ibídem.

facultado para ello, con provecho propio o de un tercero, datos personales, contenidos en ficheros, archivos, bases de datos o medios semejantes[30].

personas naturales y sanciones pecuniarias en el caso de las personas jurídicas[31].

Egipto

[Original: árabe]
[8 Abril 2022]

Capítulo II
Criminalización, procedimiento penal y aplicación de la ley

Artículo 5
Criminalización

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para prevenir y detectar la comisión de los delitos contemplados en la presente Convención o cualquier otro delito cometido a través de las tecnologías de la información y las comunicaciones, incluidos el bloqueo y la eliminación de contenido relacionado con dichos delitos, el enjuiciamiento de sus autores, la extradición de los delincuentes, la facilitación de los procedimientos de cooperación internacional y la reunión de pruebas respecto de esos delitos, al tiempo que afirme la importancia del principio de la neutralidad tecnológica.

2. Cada Estado parte adoptará también las medidas legislativas y de otra índole que resulten necesarias para criminalizar los siguientes actos:

Artículo 6
Utilización ilícita o facilitación de la utilización ilícita de los servicios y las tecnologías de la información y las comunicaciones

La utilización ilícita o la facilitación a otras personas de la utilización de los servicios de comunicación o de canales de difusión en audio o video a través de una red de información o las tecnologías de la información y las comunicaciones.

Artículo 7
Acceso ilícito o que excede los límites del derecho de acceso

1. Una persona que excede los plazos o los límites del nivel de acceso de un derecho que le hubiera sido conferido para acceder a un sitio web, una cuenta privada o un sistema informático.

2. El acceso ilícito a todo o una parte de una tecnología de la información, la presencia ilícita en esta o el contacto ilícito con esta, así como su perpetuación.

3. Se incrementará la pena si dicho acceso, presencia, contacto o perpetuación lleva a:

a) la eliminación, modificación, distorsión, copia, transferencia o destrucción de datos guardados, dispositivos o sistemas electrónicos o redes de comunicaciones o el daño a usuarios y beneficiarios;

b) la obtención de información gubernamental confidencial.

[30] Artículo 269F, Ley 1773 de 2009.
[31] Artículo 13 del Convenio de Budapest sobre la Ciberdelincuencia. En consonancia con el artículo 30 de la Convención de las Naciones Unidas contra la Corrupción y el artículo 11 de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional.

Artículo 8
Ataques al diseño de un sitio

El daño, perturbación, ralentización, distorsión, ocultación o modificación ilícitos del diseño del sitio de una empresa, institución, establecimiento o persona física.

Artículo 9
Interceptación ilícita

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

Artículo 10
Ataques a la integridad de los datos

La destrucción, eliminación, obstrucción, modificación o bloqueo deliberados e ilícitos de datos de la tecnología de la información.

Artículo 11
Uso indebido de la tecnología de la información

La producción, venta, compra, importación, distribución, suministro o posesión de cualquier herramienta o programa informático concebido o adaptado, contraseña o información similar que permita acceder a un sistema de información con la intención de que sea utilizado para cometer un delito previsto en la presente Convención, o la creación de programas informáticos maliciosos destinados a destruir, bloquear, modificar, copiar o diseminar información digital o neutralizar las funciones de seguridad de la información digital, excepto con fines de investigación legítima.

Artículo 12
Falsificación

La utilización de la tecnología de la información para cambiar la sustancia de los datos con la intención de utilizar los datos como datos válidos de modo que ocasione daños.

Artículo 13
Fraude

El daño deliberado e ilícito causado a los beneficiarios y usuarios con la intención fraudulenta de realizar derechos y beneficios por vías ilícitas para el autor u otra persona, también mediante delitos electrónicos fraudulentos relacionados con las monedas virtuales (digitales o encriptadas).

Artículo 14
Amenaza y chantaje

La utilización de las tecnologías de la información y las comunicaciones o cualquier otro medio técnico para amenazar o chantajear a una persona a fin de que cometa un acto o se abstenga de cometer un acto.

Artículo 15
Pornografía

1. La producción, exhibición, distribución, suministro, publicación, compra, venta o importación de material pornográfico con fines de prostitución o explotación de mujeres o menores a través de las tecnologías de la información y las comunicaciones, de conformidad con el derecho interno de cada Estado.

2. La producción, exhibición, distribución, suministro, publicación, compra, venta o importación de material pornográfico que represente a niños o menores, incluida la posesión de material que represente a niños o menores y que sea considerado obsceno,

a través de las tecnologías de la información y las comunicaciones o un medio que permita almacenar las tecnologías de la información y las comunicaciones.

Artículo 16
Otros delitos relacionados con la pornografía

La explotación o acoso sexual, especialmente de mujeres, niños o menores.

Artículo 17
Incitación o coacción para cometer suicidio

La incitación o coacción, también de menores, para cometer suicidio, mediante presión psicológica o de otra índole en las redes de información y las comunicaciones, inclusive Internet, ya sea a través de la interacción directa o a través de tecnologías modernas y juegos electrónicos.

Artículo 18
Implicación de menores en la comisión de actos ilícitos

La implicación de menores, a través de las tecnologías de la información y las comunicaciones, en la comisión de actos ilícitos que ponen en peligro su vida o su salud física o mental.

Artículo 19
Violación de la privacidad

La violación de la privacidad utilizando las tecnologías de la información y las comunicaciones, incluidas la creación de un correo electrónico, sitio web o cuenta privada y su falsa atribución a una persona física o jurídica.

Artículo 20
Delitos relacionados con el terrorismo cometidos utilizando la tecnología de la información

1. La diseminación, defensa o justificación de las ideas y los principios de grupos terroristas.

2. La financiación o la formación para la comisión de actos terroristas, la facilitación de la comunicación entre organizaciones terroristas o la prestación de apoyo logístico a los autores de actos terroristas.

3. La diseminación de métodos para elaborar explosivos empleados en particular en actos terroristas.

4. La propagación de la conflictividad, la sedición, el odio o el racismo.

5. Los Estados adoptarán las medidas necesarias para prevenir la diseminación del contenido de esa índole a través de las tecnologías de la información y las comunicaciones, incluido el bloqueo o la eliminación del contenido relacionado con esos delitos.

Artículo 21
Delitos financieros, incluido el blanqueo de dinero

1. La utilización de las tecnologías de la información y las comunicaciones para cometer delitos financieros o el uso indebido de monedas virtuales (digitales y encriptadas).

2. La realización de operaciones de blanqueo de dinero, la petición de asistencia para realizar operaciones de blanqueo de dinero o la publicación de métodos para blanquear dinero.

Artículo 22
Uso ilícito de instrumentos electrónicos de pago

1. La falsificación, fabricación o instalación de cualquier dispositivo o material que facilite la falsificación o imitación de instrumentos electrónicos de pago por cualquier medio.

2. La apropiación, utilización o suministro a otras personas de los datos de cualquier instrumento de pago o la facilitación de la obtención por otras personas de dichos datos.

3. La utilización de una red de información o la tecnología de la información para tener acceso no autorizado a los números o los datos de cualquier instrumento de pago.

4. La aceptación a sabiendas de un instrumento de pago falsificado.

Artículo 23
Delitos relacionados con la delincuencia organizada o transnacional cometidos utilizando la tecnología de la información

1. La promoción o el tráfico de estupefacientes o sustancias sicotrópicas.

2. La distribución ilícita de medicinas o productos médicos falsificados.

3. El tráfico de migrantes.

4. La trata de personas o el tráfico ilícito de órganos humanos.

5. El comercio ilícito de armas.

6. El tráfico ilícito de bienes culturales.

Artículo 24
Delitos relacionados con la infracción de los derechos de autor o derechos afines

La violación de los derechos de autor o los derechos afines, tal y como se definen en la ley del Estado parte, si la violación se comete deliberadamente.

Artículo 25
Acceso no autorizado a una infraestructura de información crítica

1. La creación, distribución o utilización de programas informáticos u otra información digital concebida para dar acceso no autorizado a una infraestructura de información crítica, incluidos la destrucción, el bloqueo, la modificación o la copia de la información contenida en ella o la neutralización de las funciones de seguridad.

2. La violación de las normas de utilización de los medios concebidos para almacenar, procesar o transferir información digital protegida presente en una infraestructura de información o en sistemas de información críticos de conformidad con el derecho interno del Estado parte, en redes de información y comunicaciones que pertenecen a una infraestructura de información crítica o los medios para acceder a ellas, si dicha violación daña la infraestructura de información crítica.

Artículo 26
Incitación a las actividades subversivas o armadas u otros delitos

Los llamamientos hechos a través de las tecnologías de la información y las comunicaciones para defender el sabotaje o las actividades armadas dirigidas contra el régimen de otro Estado que desestabilizarían la seguridad pública y la estabilidad o la comisión de delitos castigados con penas de privación de libertad de al menos un año.

Artículo 27
Delitos relacionados con el extremismo

La distribución de materiales que hacen un llamamiento a realizar actos ilícitos con una motivación política, ideológica, social o étnica o cualquier otro acto ilícito que defienda el odio étnico o religioso o la hostilidad en general, por medio de las

tecnologías de la información y la comunicaciones, o la defensa, la justificación o el suministro de acceso a ellos.

Artículo 28
Tentativa de comisión o participación en la comisión de un delito

La tentativa de comisión o la comisión de un delito tipificado en la Convención o la participación como cómplice en un delito tipificado en la Convención o la organización o la impartición de instrucciones a otras personas para que cometan un delito tipificado en la Convención.

Artículo 29
Otros actos ilícitos

La Convención no impedirá que un Estado parte criminalice otros actos ilícitos cometidos deliberadamente a través de las tecnologías de la información y las comunicaciones.

Artículo 30
Responsabilidad de las personas jurídicas

1. Cada Estado parte se compromete, con arreglo a su derecho interno, a regular la responsabilidad penal de las personas jurídicas por los delitos cometidos por sus representantes en nombre de aquellas o por cuenta de aquellas, sin perjuicio de la sanción de las personas físicas, incluidos los administradores de los sitios, que cometan los delitos.

2. Sin perjuicio de las disposiciones de la presente Convención, los proveedores de servicios y los administradores de sitios y sus afiliados tendrán las siguientes obligaciones, cuyo incumplimiento se considerará delito:

a) guardar y almacenar los siguientes datos en un registro del sistema de información o un registro de la tecnología de la información durante un período de (por determinar):

- datos que permitan identificar a los usuarios del servicio;
- datos relacionados con el contenido que se procesa en sistemas de información cuando dichos datos se encuentran bajo el control del proveedor de servicios;
- datos relacionados con el tráfico de comunicación;
- datos relacionados con los periféricos de comunicación;
- cualquier otro dato especificado por el Estado a los efectos de aplicar la presente Convención;

b) mantener la confidencialidad de los datos guardados y almacenados y abstenerse de revelar los datos sin que medie una orden motivada de las autoridades competentes, incluidos los datos personales de cualquiera de sus usuarios de servicios, cualquier dato o información relacionada con los sitios y las cuentas privadas a que acceden sus usuarios y las personas o entidades con que se comunican sus usuarios;

c) asegurar los datos y la información de manera tal que mantenga su confidencialidad e impida que se penetren o dañen los datos y la información;

d) brindar acceso fácil, directo y continuo a los datos y la información siguiente a los usuarios de sus servicios y a cualquier autoridad competente:

- el nombre y la dirección del proveedor de servicios;
- la información de contacto del proveedor de servicios, incluida su dirección de correo electrónico;
- los datos de licencia que identifiquen al proveedor de servicios y la autoridad competente que lo supervisa;

e) suministrar, a petición de las autoridades competentes especificadas por el Estado, todas las capacidades técnicas necesarias para que dichas autoridades puedan ejercer sus facultades.

El Salvador

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

Disposiciones sobre la penalización

Los Estados deberán adoptar las medidas legislativas y de otra índole pertinentes con vistas a reconocer como delito con arreglo a su legislación nacional, imponiendo las sanciones penales y de otra índole, inclusive privación de libertad, que tengan en cuenta la cantidad de víctimas y la cuantía del daño causado, para los siguientes casos:

Acceso ilegal

Cuando sea cometido intencionalmente, el acceso a todo o parte de un sistema informático sin el debido derecho. Se exceptúan las pruebas autorizadas o actividades de investigación legítimas y que sean verificables, siempre y cuando no produzcan daños colaterales graves.

Interceptación ilícita

Cuando sea cometido de forma intencional e ilegítima, la interceptación sin el debido derecho, realizado a través de medios técnicos en transmisiones no públicas de datos informáticos, dirigidas a un sistema informático, desde un sistema informático o dentro de este, incluyendo las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos.

Interferencia de datos

Cuando sea cometido de forma intencional e ilegítima, el daño, borrado, deterioro, alteración o supresión de datos informáticos sin el derecho correspondiente.

Interferencia a sistemas informáticos

Cuando sea cometido de forma intencional e ilegítima, la obstaculización grave al funcionamiento de un sistema informático, mediante la introducción, transmisión, daño, eliminación, deterioro, alteración o supresión de datos informáticos.

Abuso de los dispositivos

Cuando sea cometido de forma intencional e ilegítima, la producción, venta, adquisición para el uso, importación, distribución o puesta a disposición de cualquier dispositivo, incluidos programas de computadora, diseñado o adaptado principalmente con el fin de cometer cualquiera de los delitos establecidos en esta convención, así como contraseñas, códigos de acceso o datos similares por medio de los cuales se puede acceder a todo o parte de un sistema informático, con el fin de cometer cualquiera de los delitos establecidos en esta convención. Se exceptúan las pruebas autorizadas, actividades de investigación legítimas y que sean verificables, siempre y cuando no produzcan daños colaterales graves.

Falsificación informática

Cuando sea cometida, la introducción, alterado, borrado o supresión deliberados e ilegítimos de datos informáticos que generen datos no auténticos, independientemente que los datos sean legibles e inteligibles directamente. Se podrá exigir que exista una intención dolosa delictiva similar para que se considere que existe responsabilidad penal.

Fraude con la utilización de las tecnologías de la información y las comunicaciones

Cuando sea cometido deliberada e ilegítimamente, actos que causen perjuicio patrimonial a otra persona a través de cualquier entrada, alteración, eliminación o supresión de datos informáticos, o cualquier interferencia con el funcionamiento de un sistema informático con intenciones fraudulentas o deshonestas de procurar un beneficio económico para él mismo o para una tercera persona.

Delitos relacionados con material con contenido de abuso infantil

Cuando sea cometido de manera deliberada e ilegítima, las siguientes conductas: el producir, reproducir, distribuir, publicar, importar, exportar, ofrecer, financiar, vender, comercializar, difundir o poseer dichos contenidos en cualquier tipo de dispositivo o medio tecnológico.

Infracción de la propiedad intelectual y derechos afines

Cuando sea cometido, la infracción de la propiedad intelectual y derechos afines, tal y como se definen en la legislación del Estado parte, cuando estos hechos son cometidos premeditadamente con la utilización de la tecnología de la información y las comunicaciones, inclusive el uso ilícito de los programas informáticos y bases de datos, que son objetos de derecho de autor, y la apropiación de la autoría.

Complicidad en delito y tentativa de delito

La participación a cualquier título, como cómplice, asistente o instigador, en un delito; toda tentativa de cometer un delito o la preparación para un delito tipificado de conformidad con la presente convención.

Responsabilidades

Cada Estado parte adoptará las medidas que sean necesarias, de conformidad con sus principios jurídicos, para establecer la responsabilidad de una persona jurídica por la participación en delitos tipificados en la presente convención, cuando sean cometidos por cuenta de esta por una persona física, ya sea a título individual o como miembro de un órgano de dicha persona jurídica, que ejerza funciones directivas en su seno, en virtud de: un poder de representación de la persona jurídica, una autorización para tomar decisiones en nombre de la persona jurídica o una autorización para ejercer funciones de control en el seno de la persona jurídica.

Además de los casos previstos en el párrafo anterior, cada Estado parte adoptará las medidas necesarias para que pueda exigirse responsabilidad a una persona jurídica, cuando la ausencia de vigilancia o de control por parte de cualquier persona física mencionada en el párrafo anterior haya permitido la comisión de un delito previsto en aplicación de la presente convención por una persona física que actúe por cuenta de la persona jurídica y bajo su autoridad.

Dependiendo de los principios jurídicos, tal responsabilidad podrá ser penal, civil o administrativa. Dicha responsabilidad se entenderá sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido los delitos.

Cada Estado parte garantizará, en particular, que las personas jurídicas consideradas responsables de conformidad con la presente convención estén sujetas a sanciones penales o no penales efectivas, proporcionadas y disuasorias, incluidas sanciones pecuniarias.

Enjuiciamiento, adjudicación y sanciones

Cada Estado parte hará que la comisión de un delito tipificado de conformidad con los artículos de la presente convención esté sujeta a sanciones que tengan en cuenta la gravedad de ese delito.

Cada Estado parte se esforzará por garantizar que cualquier facultad legal discrecional en virtud de su derecho interno en relación con el enjuiciamiento de

personas por delitos comprendidos en la presente convención se ejerza para maximizar la eficacia de las medidas de aplicación de la ley con respecto a esos delitos y teniendo debidamente en cuenta la necesidad para disuadir la comisión de tales delitos.

En el caso de delitos tipificados de conformidad con los artículos de la presente convención, cada Estado parte tomará las medidas apropiadas, de conformidad con su derecho interno y teniendo debidamente en cuenta los derechos de defensa, para solicitar garantizar que las condiciones impuestas en relación con las decisiones sobre la puesta en libertad en espera de juicio o apelación tengan en cuenta la necesidad de garantizar la presencia del acusado en los procesos penales posteriores.

Cada Estado parte se asegurará de que sus tribunales u otras autoridades competentes tengan en cuenta la gravedad de los delitos comprendidos en la presente convención al considerar la eventualidad de la libertad anticipada o la libertad condicional de las personas condenadas por tales delitos.

Cada Estado parte establecerá, cuando corresponda, en su derecho interno, un plazo de prescripción prolongado para iniciar un proceso por cualquier delito comprendido en la presente convención y un plazo más prolongado cuando el presunto infractor haya eludido la administración de justicia.

Nada de lo contenido en esta convención afectará el principio de que la descripción de los delitos establecidos de acuerdo con la presente convención y de las excepciones legales aplicables u otros principios legales que rigen la legalidad de la conducta se reservan al derecho interno de un Estado parte y que tal los delitos serán perseguidos y castigados de conformidad con esa ley.

Lavado de activos resultados de delitos con el uso de las tecnologías de la información y las comunicaciones

Cada Estado parte adoptará, de conformidad con los principios fundamentales de su derecho interno, las medidas legislativas y de otra índole que sean necesarias para tipificar como delitos penales, cuando se cometan intencionalmente los siguientes:

a) La conversión o transferencia de bienes, a sabiendas de que tales bienes son producto del delito, con el fin de ocultar o encubrir el origen ilícito de los bienes o de ayudar a cualquier persona que esté involucrada en la comisión del delito determinante a eludir las consecuencias legales de sus acciones.

b) El ocultar o disfrazar de la verdadera naturaleza, fuente, ubicación, disposición, movimiento o propiedad o derechos con respecto a la propiedad, sabiendo que dicha propiedad es producto del delito.

c) La adquisición, posesión o uso de bienes, sabiendo, en el momento de su recepción, que tales bienes son producto del delito.

d) La participación en, asociación o conspiración para cometer, intentos de cometer y ayudar, instigar, facilitar y aconsejar la comisión de cualquiera de los delitos establecidos de conformidad con la presente convención.

A los efectos de implementar o aplicar lo indicado en este párrafo, cada Estado parte procurará lo siguiente:

a) Aplicar lo indicado en este párrafo a la gama más amplia de delitos determinantes;

b) Incluir como delitos determinantes los delitos tipificados de conformidad con los artículos de la presente convención. En el caso de los Estados partes cuya legislación establezca una lista de delitos determinantes específicos, deberán, como mínimo, incluir en dicha lista una amplia gama de delitos relacionados con grupos delictivos organizados;

c) Para los efectos del subpárrafo anterior b), los delitos determinantes incluirán los delitos cometidos tanto dentro como fuera de la jurisdicción del Estado parte en cuestión. Sin embargo, los delitos cometidos fuera de la jurisdicción de un Estado parte

constituirán delitos determinantes únicamente cuando la conducta en cuestión sea un delito penal conforme al derecho interno del Estado donde se comete y sería un delito penal conforme al derecho interno del Estado parte que implementa o aplica este artículo si se hubiera cometido allí;

d) Cada Estado parte proporcionará copias de sus leyes que dan efecto a este artículo y de cualquier cambio posterior a dichas leyes o una descripción de estos al Secretario General de las Naciones Unidas.

Obstrucción a la justicia

Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delitos penales, cuando se cometan intencionalmente, los siguientes:

a) el uso de la fuerza física, las amenazas o la intimidación o la promesa, el ofrecimiento o la entrega de una ventaja indebida para inducir a falso testimonio o interferir en la prestación de testimonio o la producción de pruebas en un proceso en relación con la comisión de los delitos comprendidos en esta convención;

b) el uso de la fuerza física, las amenazas o la intimidación para interferir en el ejercicio de las funciones oficiales de un funcionario judicial o encargado de hacer cumplir la ley en relación con la comisión de los delitos comprendidos en la presente convención. Nada de lo dispuesto en este inciso perjudicará los derechos de los Estados partes a contar con legislación que proteja a otras categorías de funcionarios públicos.

Jurisdicción

Cada Estado parte adoptará las medidas que sean necesarias para establecer su jurisdicción sobre los delitos tipificados de conformidad con la presente convención cuando:

a) el delito se comete en el territorio de ese Estado parte;

b) el delito se comete a bordo de una embarcación que enarbole el pabellón de ese Estado parte o de una aeronave que esté matriculada conforme a las leyes de ese Estado parte en el momento en que se comete el delito;

Un Estado parte también podrá establecer su jurisdicción sobre cualquiera de esos delitos cuando:

a) el delito se comete contra un nacional de ese Estado parte;

b) el delito es cometido por un nacional de ese Estado parte o un apátrida que tenga su residencia habitual en su territorio;

c) el delito es cometido contra un Estado parte.

Cada Estado parte tomará las medidas que sean necesarias para establecer su jurisdicción sobre los delitos tipificados de conformidad con la presente convención cuando el presunto delincuente se encuentre en su territorio y no extradite a esa persona únicamente por el hecho de que es uno de sus nacionales.

Si un Estado parte que ejerce su jurisdicción de conformidad con los párrafos anteriores y ha sido notificado, o se ha enterado de otro modo, de que cualquier otro Estado parte está realizando una investigación, enjuiciamiento o procedimiento judicial con respecto a la misma conducta, las autoridades competentes de esos Estados partes se consultarán, según corresponda, con miras a coordinar sus acciones.

Sin perjuicio de las normas del derecho internacional general, la presente convención no excluirá el ejercicio de la jurisdicción penal establecida por un Estado parte de conformidad con su derecho interno.

Unión Europea y sus Estados miembros

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

Capítulo II
Criminalización y aplicación de la ley

Artículo 5
Acceso ilícito

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

2. Los Estados partes podrán exigir que el delito se cometa con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático.

Artículo 6
Interceptación ilícita

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro de este, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos.

2. Los Estados partes podrán exigir que el delito se cometa con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

Artículo 7
Ataques a la integridad de los datos

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos.

2. Los Estados partes podrán exigir que los actos descritos en el párrafo 1 comporten daños graves.

Artículo 8
Ataques ilícitos a la integridad del sistema

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

Artículo 9
Uso indebido de los dispositivos

1. Cada Estado Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito la comisión deliberada e ilegítima de los siguientes actos:

a) la producción, venta, obtención para su utilización, importación, distribución o cualquier otra forma de puesta a disposición de:

i) cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos tipificados con arreglo a los artículos 5 a 8 de la presente Convención;

ii) una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático;

con intención de que sean utilizados para cometer cualquiera de los delitos tipificados con arreglo a los artículo 5 a 8 de la presente Convención, y

b) la posesión de alguno de los elementos contemplados en los incisos i) o ii) del apartado a) del presente párrafo, con intención de que sean utilizados para cometer cualquiera de los delitos tipificados con arreglo a los artículos 5 a 8 de la presente Convención. Los Estados partes podrán exigir la posesión de un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

2. No se interpretará que el presente artículo impone responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, distribución o cualquier otra forma de puesta a disposición o la posesión mencionada en el párrafo 1 del presente artículo no tenga por objeto la comisión de uno de los delitos tipificados con arreglo a los artículos 5 a 8 de la presente Convención, como en el caso de las pruebas autorizadas o de la protección de un sistema informático.

3. Los Estados partes podrán no aplicar el párrafo 1 del presente artículo, siempre que no afecte a la venta, distribución o cualquier otra forma de puesta a disposición de los elementos mencionados en el inciso ii) del párrafo 1 a) del presente artículo.

Artículo 10
Tentativa y complicidad

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito cualquier complicidad deliberada con vistas a la comisión de alguno de los delitos tipificados con arreglo a los artículos 5 a 9 de la presente Convención.

2. Cada Estado parte podrá adoptar las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito toda tentativa deliberada de cometer alguno de los delitos tipificados con arreglo a los artículos 5 a 9 de la presente Convención.

Artículo 11
Responsabilidad de las personas jurídicas

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias, en consonancia con sus principios jurídicos, para que pueda exigirse responsabilidad a una persona jurídica por los delitos tipificados con arreglo a los artículos 5 a 10 de la presente Convención.

2. Dependiendo de los principios jurídicos de cada Parte, la responsabilidad de una persona jurídica podrá ser penal, civil o administrativa.

3. Dicha responsabilidad se entenderá sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido los delitos.

Artículo 12
Proceso, fallo y sanciones

1. Cada Estado parte penalizará la comisión de los delitos tipificados con arreglo a los artículos 5 a 10 de la presente Convención imponiendo sanciones efectivas, proporcionadas y disuasorias tanto a las personas físicas como a las personas jurídicas.

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

3. Cada Estado parte establecerá y mantendrá un sistema nacional de justicia penal eficaz y basado en el estado de derecho que pueda garantizar que toda persona enjuiciada

por los delitos comprendidos en la presente Convención sea sometida a la acción de la justicia al tiempo que se protegen plenamente los derechos humanos y las libertades fundamentales, incluido el derecho a un juicio imparcial y el derecho a la defensa.

Ghana

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

Capítulo II. Disposiciones relativas a la criminalización[32]

Delitos basados en la cibernética: delitos contra la confidencialidad, la integridad y la disponibilidad de los sistemas y datos informáticos

Artículo 5
Acceso no autorizado a un sistema informático

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito el acceso deliberado a todo o parte de un sistema informático sin autorización o excediendo el acceso autorizado. Las Partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

Artículo 6
Acceso no autorizado a una infraestructura de información crítica

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito el acceso deliberado a todo o parte de una infraestructura de información crítica sin autorización.

Artículo 7
Interceptación no autorizada

Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada y sin autorización, por medios técnicos, de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro de este, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos.

Las Partes podrán exigir que el delito se cometa con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

Artículo 8
Ataques a la integridad de los datos

1. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado y sin autorización que dañe, borre, deteriore, altere, copie o suprima datos informáticos.

2. Las Partes podrán reservarse el derecho a exigir que los actos descritos en el párrafo 1 comporten daños graves.

[32] El texto de esta sección se basa fundamentalmente en el Convenio del Consejo de Europa sobre la Ciberdelincuencia, la Convención de la Unión Africana sobre la Ciberseguridad y la Protección de los Datos Personales, la Ley de Transacciones Electrónicas de 2008 (Ley 772) y la Ley de Ciberseguridad de 2020 (Ley 1038). Estos instrumentos conforman el marco legislativo de Ghana en materia de ciberdelincuencia.

Artículo 9
Ataques a la integridad del sistema

Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada y sin autorización del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

Artículo 10
Uso indebido de los dispositivos

1. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a) la producción, venta, obtención para su utilización, importación, distribución o cualquier otra forma de puesta a disposición de:

i) cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos tipificados con arreglo a los artículos 5 a 9;

ii) una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con intención de que sean utilizados para cometer cualquiera de los delitos tipificados con arreglo a los artículos 5 a 9, y

b) la posesión de alguno de los elementos contemplados en los incisos i) o ii) del apartado a) del presente párrafo, con intención de que sean utilizados para cometer cualquiera de los delitos tipificados con arreglo a los artículos 5 a 9. Las Partes podrán exigir en su derecho interno la posesión de un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

2. No se interpretará que el presente artículo impone responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, distribución o cualquier otra forma de puesta a disposición o la posesión mencionada en el párrafo 1 del presente artículo no tenga por objeto la comisión de uno de los delitos tipificados con arreglo a los artículos 5 a 9 de la presente Convención, como en el caso de las pruebas autorizadas o de la protección de un sistema informático.

3. Las Partes podrán reservarse el derecho a no aplicar el párrafo 1 del presente artículo, siempre que dicha reserva no afecte a la venta, distribución o cualquiera otra forma de puesta a disposición de los elementos mencionados en el inciso ii) del párrafo 1 a) del presente artículo.

Delitos facilitados por la cibernética: delitos cuyo alcance, velocidad y efectos pueden haber aumentado a raíz de la llegada de los[33]

Artículo 11
Falsificación informática

Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente. Las Partes podrán exigir que exista una intención fraudulenta o delictiva similar para que se considere que existe responsabilidad penal.

[33] El fraude informático, la falsificación informática y los delitos contra los niños están en consonancia con el Convenio del Consejo de Europa sobre la Ciberdelincuencia, la Convención de la Unión Africana sobre la Ciberseguridad y la Protección de los Datos Personales y la Ley de Ciberseguridad de 2020 (Ley 1038).

Artículo 12
Fraude informático

Cada Parte adoptará las medidas legislativas o de otra índole que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante:

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

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

con la intención fraudulenta o delictiva de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.

Delitos contra los niños

Artículo 13
Delitos relacionados con la explotación y los abusos sexuales de niños en línea

1. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a) la producción de material que muestre explotación y abusos sexuales de niños con la intención de publicarlo y distribuirlo a través de un sistema informático;

b) la obtención, para uno mismo o para otra persona, de material que muestre explotación y abusos sexuales de niños;

c) la oferta o la puesta a disposición de material que muestre explotación y abusos sexuales de niños a través de un sistema informático o un dispositivo electrónico;

d) la publicación, distribución, emisión en línea (incluida la emisión en directo) y transmisión de material que muestre explotación y abusos sexuales de niños a través de una computadora o un dispositivo electrónico, o

e) la posesión de material que muestre explotación y abusos sexuales de niños en un sistema informático o un dispositivo informático o electrónico de almacenamiento de grabaciones.

2. A los efectos del apartado c) del párrafo 1, una persona publica material que muestre explotación y abusos sexuales de niños si dicha persona

a) entrega a otra persona la posesión del material que muestre explotación y abusos sexuales de niños, o

b) expone u ofrece el material que muestre explotación y abusos sexuales de niños para su adquisición por otra persona.

3. A los efectos del presente artículo, quedan comprendidas dentro de “material que muestre explotación y abusos sexuales de niños”, entre otras cosas, imágenes materiales, grabaciones visuales, videos, archivos de audio, materiales de emisión en directo, dibujos o escritos que representen o describan:

a) a un niño adoptando un comportamiento sexualmente explícito o sugerente;

b) a una persona que parezca un niño adoptando un comportamiento sexualmente explícito o sugerente;

c) imágenes que representen a un niño adoptando un comportamiento sexualmente explícito o sugerente;

d) imágenes sexualmente explícitas de niños;

e) procesos o material para ver la explotación y los abusos sexuales de niños en tiempo real, que a menudo implican que el delincuente ordene los abusos;

f) cualquier material escrito, representación visual o grabación de audio que defienda o aconseje la actividad sexual ilícita con niños;

g) cualquier material escrito que tenga, como característica dominante, la descripción, con fines sexuales, de actividades sexuales ilícitas con un niño;

h) cualquier grabación de audio que tenga, como característica dominante, la descripción, con fines sexuales, de actividades sexuales ilícitas con un niño.

Artículo 14
Interacción con un niño con fines de abuso sexual

Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la utilización deliberada de:

a) un servicio informático en línea;

b) un servicio de Internet;

c) un servicio local de tablón de anuncios, o

d) cualquier otro dispositivo que pueda almacenar o transmitir datos electrónicos,

para seducir, instigar, tentar, captar o atraer o tratar de seducir, instigar, tentar, captar o atraer a un niño o a otra persona que el autor crea que es un niño con el fin de facilitar, alentar, ofrecer o instigar conductas sexuales ilícitas de un niño o con un niño o la representación visual de dichas conductas.

Artículo 15
Ciberhostigamiento de un niño

Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la utilización deliberada de un servicio informático en línea, un servicio de Internet o un servicio local de tablón de anuncios o cualquier otro dispositivo electrónico para recopilar, transmitir, publicar, reproducir, comprar, vender, recibir, intercambiar o diseminar el nombre, número de teléfono, dirección de correo electrónico, dirección física, fotografía, descripción física, características o cualquier otra información que identifique a un niño con el objetivo de tratar de concertar un encuentro con el niño con el fin de mantener relaciones sexuales, adoptar una conducta sexualmente explícita o realizar actividades sexuales ilícitas.

Otros delitos sexuales en línea[34]

Artículo 16
Extorsión sexual

1. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la amenaza deliberada de distribuir por correo postal, enviar por correo electrónico, enviar en mensajes o transmitir, por medios electrónicos o por otras vías, una imagen privada o imágenes en movimiento de otra persona adoptando un comportamiento sexualmente explícito, con la intención específica de:

a) acosar, amenazar, coaccionar, intimidar o ejercer influencia indebida sobre la persona especialmente para extorsionarla a cambio de dinero u otra contraprestación u obligar a la víctima a realizar actividades sexuales no deseadas, o

b) extorsionar de manera efectiva a cambio de dinero u otra contraprestación u obligar a la víctima a realizar actividades sexuales no deseadas.

2. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la amenaza deliberada de distribuir por correo postal, enviar por correo electrónico, enviar en mensajes o transmitir, por medios electrónicos o por otras vías, una imagen privada o imágenes en

[34] Compatibles con las disposiciones de la Ley de Ciberseguridad.

movimiento de un niño adoptando un comportamiento sexualmente explícito, con la intención específica de:

a) acosar, amenazar, coaccionar, intimidar o ejercer influencia indebida sobre el niño especialmente para extorsionarlo a cambio de dinero u otra contraprestación u obligar a la víctima a realizar actividades sexuales no deseadas, o

b) extorsionar de manera efectiva a cambio de dinero u otra contraprestación u obligar a la víctima a realizar actividades sexuales no deseadas.

3. A los efectos de los párrafos 1 y 2, una imagen íntima podrá consistir en una representación en que la región genital o anal de otra persona esté al descubierto o cubierta únicamente con ropa interior o se muestren los pechos por debajo del borde superior de la areola, que se encuentra al descubierto o es claramente visible a través de la ropa.

Artículo 17
Difusión no consentida de imágenes íntimas

1. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la distribución deliberada de la imagen íntima o la grabación visual prohibida de otra persona identificable o el acto deliberado de hacer que otra persona la distribuya, sin el consentimiento de la persona que aparece en la imagen íntima, con la intención de causarle graves problemas emocionales, y respecto de la cual había una expectativa razonable de privacidad en el momento de creación de la imagen o grabación visual, el momento de la comisión del delito o en ambos momentos.

2. A los efectos del presente artículo, queda comprendido dentro de “graves problemas emocionales”, entre otras cosas, el comportamiento deliberado que genera reacciones mentales como el miedo, el nerviosismo, la aflicción, la ansiedad, la preocupación, la mortificación, la conmoción, la humillación y la pérdida de dignidad, así como el dolor físico.

Artículo 18
Amenaza de distribuir imágenes o grabaciones visuales íntimas prohibidas

Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la amenaza deliberada de distribuir una imagen o grabación visual íntima prohibida de otra persona de forma tal que le causaría problemas razonablemente en todas las circunstancias, cuando la amenaza se vierta de forma tal que infundiría en la otra persona el temor, razonablemente en todas las circunstancias, de que se cumpliera la amenaza.

Artículo 19
Delitos relacionados con infracciones de los derechos de autor y derechos afines[35]

1. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno las infracciones de los derechos de autor, según se definan en su legislación, de conformidad con las obligaciones que haya contraído en aplicación del Acta de París de 24 de julio de 1971 por la cual se revisó el Convenio de Berna para la Protección de las Obras Literarias y Artísticas, del Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual Relacionados con el Comercio y del Tratado de la Organización Mundial de la Propiedad Intelectual (OMPI) sobre Derecho de Autor, a excepción de cualquier derecho moral otorgado por dichos tratados, cuando tales actos se cometan intencionalmente, a escala comercial y por medio de un sistema informático.

2. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno las infracciones de los

[35] Compatibles con el Convenio del Consejo de Europa sobre la Ciberdelincuencia y la Convención de la Unión Africana sobre la Ciberseguridad y la Protección de los Datos Personales.

derechos afines, según se definan en su legislación, de conformidad con las obligaciones que haya asumido en aplicación de la Convención Internacional para la Protección de los Artistas, Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión (Convención de Roma), del Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio y del Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas, a excepción de cualquier derecho moral conferido por dichos tratados, cuando tales actos se cometan intencionalmente, a escala comercial y por medio de un sistema informático.

3. En circunstancias limitadas, toda Parte podrá reservarse el derecho de no imponer responsabilidad penal en virtud de los párrafos 1 y 2 del presente artículo, siempre que se disponga de otros recursos efectivos y que dicha reserva no vulnere las obligaciones internacionales que incumban a dicha Parte en aplicación de los instrumentos internacionales mencionados en los párrafos 1 y 2 del presente artículo.

Artículo 20
Tentativa y complicidad

1. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno cualquier complicidad deliberada con vistas a la comisión de alguno de los delitos tipificados con arreglo a los artículos 5 a 19 de la presente Convención, con la intención de que dicho delito sea cometido.

2. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno toda tentativa deliberada de cometer alguno de los delitos tipificados con arreglo a los artículos 7 a 9; 11; 12; 13, párrafo 1, apartados a), b) y e); 14; 15; 16, y 17.

Artículo 21
Responsabilidad de las personas jurídicas

1. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para que pueda exigirse responsabilidad a una persona jurídica por los delitos tipificados con arreglo a la presente Convención, cuando sean cometidos por cuenta de esta por una persona física, ya sea a título individual o como miembro de un órgano de dicha persona jurídica, que ejerza funciones directivas en su seno, en virtud de:

a) un poder de representación de la persona jurídica;

b) una autorización para tomar decisiones en nombre de la persona jurídica;

c) una autorización para ejercer funciones de control en el seno de la persona jurídica.

2. Además de los casos previstos en el párrafo 1 del presente artículo, cada Parte adoptará las medidas necesarias para garantizar que pueda exigirse responsabilidad a una persona jurídica cuando la ausencia de vigilancia o de control por parte de cualquier persona física mencionada en el párrafo 1 haya permitido la comisión de un delito tipificado con arreglo a la presente Convención por una persona física que actúe por cuenta de dicha persona jurídica y bajo su autoridad.

3. Dependiendo de los principios jurídicos de cada Parte, la responsabilidad de una persona jurídica podrá ser penal, civil o administrativa.

4. Dicha responsabilidad se entenderá sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido el delito.

Artículo 22
Sanciones y medidas

1. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para que los delitos tipificados con arreglo a los artículos 5 a 20 estén sujetos

a sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad.

2. Las Partes garantizarán la imposición de sanciones o medidas penales o no penales efectivas, proporcionadas y disuasorias, incluidas sanciones pecuniarias, a las personas jurídicas consideradas responsables de conformidad con el artículo 21.

Irán (República Islámica del)

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

2. Criminalización

Es cada vez más frecuente que los delincuentes organicen y cometan actos ilícitos, no solo contra dispositivos de las tecnologías de la información y las comunicaciones, sino mediante el uso de esos dispositivos. Aunque las conductas pueden tipificarse, tanto si las tecnologías de la información y las comunicaciones se utilizan indebidamente como si no, en algunos casos la gravedad de la falta u otros factores relacionados con el delito hacen necesario que se criminalice el acto ilícito cuando se cometa mediante esas tecnologías. Ello ocurre especialmente cuando el uso de las tecnologías de la información y las comunicaciones intensifica la comisión de delitos, por ejemplo, aumentando el daño que se causa a las víctimas. Por lo tanto, además de los delitos basados en las tecnologías de la información y las comunicaciones, deberían tipificarse en la convención los delitos facilitados por esas tecnologías. No obstante, desde un punto de vista jurídico, podría ser necesario adoptar un enfoque para cada caso concreto, dado que las distintas modalidades delictivas podrían presentar elementos diferenciados, así como un *actus reus* y una *mens rea* distintos. Al adoptarse medidas orientadas a tipificar conductas debería prestarse la debida atención a los principios fundamentales de los ordenamientos jurídicos nacionales.

También debería establecerse la responsabilidad de las personas jurídicas para que la respuesta a las actividades delictivas sea integral y para impedir que los delincuentes actúen libremente escondiéndose tras el velo que les proporcionan las personas jurídicas. Esas medidas deberían responsabilizar a las personas jurídicas por participar deliberadamente o a sabiendas en la comisión de los delitos que se establezcan de conformidad con la convención.

Japón

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

1. Criminalización

1.1. Delitos basados en la cibernética

1.1.1. El Japón considera que existe un consenso general en el Comité Especial respecto de la criminalización de los delitos basados en la cibernética, que son principalmente delitos que vulneran la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos. Sobre la base de este entendimiento, el Japón apoya que se tipifiquen los delitos basados en la cibernética.

1.1.2. Creemos que muchos de los actos que es necesario tipificar para afrontar los desafíos de hoy a los que todos los Estados Miembros asignan importancia, como los ataques con programas secuestrador y los ataques contra sistemas informáticos de infraestructura crítica, se encuentran comprendidos entre los delitos basados en la cibernética. Los delitos basados en la cibernética podrían incluir el acceso y la interceptación ilícitos y el ataque a la integridad de los datos o sistemas informáticos, así como el uso indebido de dispositivos, entre otros.

1.1.3. El Japón reconoce la importancia de adoptar medidas contra los ataques a los sistemas informáticos de las infraestructuras y servicios informáticos. Sin embargo, dado que ese tipo de ataques, como el hurto o la alteración de datos mediante la piratería informática, pueden considerarse comprendidos en los delitos basados en la cibernética, no es necesario tratar esos delitos como cuestiones específicas de las infraestructuras o servicios informáticos. Asimismo, habida cuenta de que es importante que la convención que se elabore pueda aplicarse en el futuro lejano, cabe destacar que las disposiciones relativas a la criminalización serán menos versátiles si se centran demasiado en el *modus operandi* de cada caso. Además, es importante que esta nueva convención establezca disposiciones fundamentales y esenciales que puedan cumplir e incorporar a su derecho interno el mayor número de Estados Miembros posible. A la luz de estas consideraciones, los debates deberían comenzar con los delitos cibernéticos comunes, como el acceso ilícito. Debería ponderarse cuidadosamente si es necesario o no establecer una disposición específica para los ataques contra los sistemas informáticos de la infraestructura y los servicios de la información, además de las disposiciones que se elaboren sobre delitos cibernéticos comunes para evitar la duplicación de las disposiciones relativas a la criminalización.

1.1.4. Además, es necesario evitar el riesgo de que se produzca un efecto de paralización de las operaciones y actividades legítimas, como el desarrollo tecnológico, o que las fuerzas del orden abusen de su poder al haberse tipificado las conductas de una manera demasiado amplia. Por ejemplo, cuando se tipifique el acceso ilícito, tal vez sea necesario establecer que no debe existir una razón legítima para el acceso y que debe estarse en conocimiento de ello para no imponer una responsabilidad objetiva.

1.1.5. Asimismo, establecer sanciones uniformes para la tentativa de cometer un delito o la complicidad en su comisión o sanciones para la preparación del delito o la confabulación para cometerlo, cuando los actos que se lleven a cabo no lleguen a constituir un delito en grado de tentativa, sería interferir excesivamente en la legislación penal de los Estados. La tipificación de esas conductas debería dejarse librada a la legislación nacional de cada Estado Miembro. En cuanto a las medidas que se adopten en contra de los delitos cibernéticos transnacionales, resulta muy importante no crear refugios seguros para la ciberdelincuencia. Por consiguiente, es necesario evitar disposiciones que tengan como consecuencia limitar el número de Estados Miembros que puedan concertar la nueva convención debido a la existencia de diferencias en los conceptos jurídicos básicos que inevitablemente existirán entre los Estados Miembros.

1.2. Libertad de expresión

1.2.1. Al considerar la tipificación de actividades en el ciberespacio, debería hacerse referencia a los tratados internacionales de derechos humanos. Al determinar qué actos pueden tipificarse como delitos facilitados por la cibernética en la nueva convención, en particular en relación con la penalización de actos relacionados con contenidos nocivos en Internet, los Estados Miembros no deben olvidar que es importante proteger la libertad de expresión.

1.2.2. Por ejemplo, el artículo 19, párrafo 2, del Pacto Internacional de Derechos Civiles y Políticos establece que la libertad de expresión “comprende la libertad de libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección”. Sin dejar de tomar en consideración lo dispuesto en el artículo 19, párrafo 3, que restringe ese derecho, debemos asegurarnos de que quede un espacio para la elaboración de leyes nacionales, teniendo en cuenta la situación actual de cada Estado Miembro, de modo que los derechos y las libertades relativas a la investigación académica, cultural y artística, y la libertad de prensa, no se vulneren injustamente.

1.2.3. Para proteger la libertad de expresión, es necesario evitar que se produzca el efecto de paralizar las actividades expresivas. Así pues, los actos relacionados con el contenido nocivo en Internet solo deberían tipificarse en la medida en que todos los

Estados Miembros puedan ponerse de acuerdo sobre la definición de esos actos, y existan fundamentos demostrables de que existe la necesidad de sancionarlos.

1.2.4. A fin de que la convención sea un tratado que puedan concertar el mayor número posible de Estados Miembros, y de esperar a que las deliberaciones maduren tanto en el ámbito internacional como nacional, creemos que una de las opciones más prometedoras sería dejar la tipificación de los actos relativos a los contenidos nocivos para un futuro protocolo adicional.

1.3. Delitos relativos a la explotación del ciberespacio previstos en convenciones

1.3.1. En cuanto a los delitos relativos al terrorismo, los delitos relacionados con las armas de fuego y los delitos relacionados con drogas, estos podrían preverse en la convención, incluso cuando se los cometa mediante el uso de Internet; es posible que también resulten aplicables tratados como la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional.

1.3.2. La tipificación de esos actos debería considerarse cuidadosamente, para no duplicar la labor de tipificación que ya se haya realizado, como se señala más arriba. También debería hacerse referencia a las deliberaciones que se han llevado a cabo durante el proceso de elaboración de los tratados vigentes para que las disposiciones que se hayan excluido deliberadamente de ellos no sean incorporadas en la convención actual de alguna otra forma.

1.4. Delitos facilitados por la cibernética que podrían considerarse

En cuanto a los delitos facilitados por la cibernética que no se relacionen con contenidos nocivos (véase el párrafo 1.2 más arriba), algunos delitos facilitados por la cibernética que se reconoce como suficientemente importantes para tipificárselos como delitos cibernéticos en esta convención podrían ser objeto de un debate sobre la criminalización, con la premisa de que todos los Estados Miembros puedan ponerse de acuerdo en una definición de esos actos y que existirán fundamentos demostrables de que existe la necesidad de sancionarlos. Esos delitos facilitados por la cibernética incluyen aquellos cuyo alcance y velocidad, así como la envergadura de los daños que provocan, se ven aumentados por el uso de computadoras. Entre esos delitos podrían incluirse los siguientes:

1.4.1. Falsificación informática

Es difícil detectar falsificaciones de datos informáticos a través de los sentidos. Además, en el mundo de hoy en que muchos de los procesos institucionales se llevan a cabo por medio de computadoras, el impacto que tiene en la sociedad el socavar la confianza en los datos informáticos es considerable. Por lo tanto, el Japón podría apoyar la tipificación de la introducción, alternación, borrado o supresión deliberados e ilegítimos de datos informáticos, que genere datos no auténticos.

1.4.2 Fraude informático

El fraude informático de datos, cuando se lo comete mediante la falsificación de datos informáticos o la interferencia en los sistemas informáticos, es fácil de perpetrar contra una amplia variedad de objetivos y puede causar daños graves a bienes en muchos Estados Miembros. Por lo tanto, podríamos apoyar que se tipifique el causar perjuicio patrimonial a otra persona mediante la introducción, alteración, borrado o supresión de datos informáticos o cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener un beneficio.

1.4.3 Infracciones de la propiedad intelectual

En Internet, es posible copiar datos y es fácil reproducir el contenido, y este último se propaga fácilmente, lo que puede aumentar el grado de la violación de los derechos de autor. Creemos que sería beneficioso que se penalizara la violación de los derechos de autor y otros derechos relacionados con estos, cuando esos actos se cometan

deliberadamente, a escala comercial y por medio de sistemas informáticos, con referencia a acuerdos internacionales vigentes relacionados con los derechos de autor.

1.4.4 Abuso y explotación sexuales de niños

La producción y distribución de material que muestra abusos sexuales de niños constituyen actos extremadamente maliciosos que tienen un efecto perjudicial en la salud mental y física de los niños que aparecen en él y vulneran gravemente sus derechos humanos. Es difícil eliminar el material que muestra abusos sexuales de niños una vez que ha sido diseminado en Internet, y ese material seguirá teniendo graves consecuencias en la crianza saludable de los niños. Desde la perspectiva de la protección de los derechos humanos de los niños, apoyamos la tipificación de la producción y distribución de material que represente visualmente a un niño adoptando un comportamiento sexualmente explícito.

Sin embargo, creemos que debería tenerse cuidado al tratar las imágenes que representan con realismo a una persona que parece ser un menor o un niño inexistente que adopta un comportamiento sexualmente explícito como material que muestra abusos sexuales de niños y tipificar delitos relacionados con esas imágenes, y debería tenerse en cuenta que en ese caso no hay un menor que exista realmente que esté siendo sometido a un abuso directo, así como la importancia de la libertad de expresión.

1.5. Responsabilidad de las personas jurídicas

Apoyamos que se establezca la responsabilidad de las personas jurídicas hasta cierto punto en los casos en que esas personas jurídicas cometieran delitos cibernéticos de forma generalizada en relación con el desarrollo de sus actividades, con la condición de que esa responsabilidad pueda ser penal, civil o administrativa, según los principios jurídicos de cada Estado Miembro. La división de funciones, en cuanto a si una cuestión es penal, civil o administrativa, así como la necesidad de imponer sanciones son cuestiones que deberían dejarse en manos de la legislación nacional de cada Estado Miembro, habida cuenta de que deben examinarse a la luz de la estructura interna de cada Estado Miembro y de la paridad que exista con la gobernanza fuera del ámbito de la cibernética en cada uno de ellos.

Jordania

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

El Reino Hachemita de Jordania propone que los siguientes actos se tipifiquen en el proyecto de convención:

- El acceso ilícito y deliberado a una red o un sistema de información o a cualquier parte de ellos por cualquier medio, o en infracción a esa autorización. La sanción para ese delito debería agravarse en los casos en que la red o el sistema de información o cualquier parte de ellos a los que se acceda ilícitamente pertenezcan a una institución oficial, pública, encargada de la seguridad, financiera o bancaria y el acceso ilícito sea a una infraestructura crítica y los datos o la información de que se trate no fueran de consulta pública y afectaran a la seguridad nacional, las relaciones exteriores del Estado, la seguridad pública o la economía nacional.
- La interceptación ilícita de tráfico de datos.
- La violación de datos o información relacionados con medios de pago electrónicos, la ejecución de operaciones bancarias o financieras o la transferencia de fondos mediante una red o sistema de información.
- El fraude electrónico.
- El fraude en las direcciones de Internet.

- La explotación sexual a través de sistemas o redes de información o sitios web.
- La difusión de rumores o noticias falsas mediante sistemas o redes de información o sitios web.
- El discurso de odio o las acciones que impliquen un insulto a religiones o Estados mediante sistemas o redes de información o sitios web.
- El ataque ilícito a la integridad de sistemas o redes de información mediante la instalación o la introducción de programas maliciosos.
- La creación de un sitio web similar a un sitio web real para inducir a error o engañar a los usuarios con el fin de robar datos de acceso o información personal o recaudar donaciones ilícitas.
- El envío de correos electrónicos o mensajes de texto con objeto suplantar la identidad (*phishing*) para robar datos, propagar programas maliciosos o intentar acceder a redes o sistemas de información a los cuales no esté permitido acceder.
- La creación de páginas, grupos o cuentas falsas en sitios de medios sociales para inducir a error o engañar a los usuarios, recaudar donaciones ilícitas o mendigar por medios electrónicos.
- Los ataques a dispositivos de usuarios para crear una red de información sin el conocimiento de los usuarios con objeto de perpetrar ataques orientados a Socavar la confianza o con otra finalidad ilícita.
- La explotación o la tentativa de explotación de vulnerabilidades en las redes o sistemas de información con la intención de penetrar en ellos o destruir o modificar datos.
- El escaneo o la tentativa de escaneo de protocolos de Internet o puertos de acceso de redes sin permiso con la intención de recolectar información o detectar vulnerabilidades en la seguridad.
- El uso no autorizado de *hardware* o *software* para adivinar contraseñas o nombres de usuario.
- El uso de la tecnología de inteligencia artificial para cometer actos ilícitos.
- Los actos relacionados con la suplantación de identidad.
- Los actos relacionados con las intrusiones a la privacidad.
- Los actos relacionados con la propiedad intelectual y la piratería informática.
- Los actos que constituyan un ataque contra las cadenas de suministro.
- Los actos relacionados con el uso no autorizado de datos por proveedores de servicios.
- Los actos relacionados con la difusión, el apoyo o la promoción de una ideología terrorista.
- Los actos relacionados con la utilización de las tecnologías de la información y las comunicaciones con fines terroristas.
- Los actos relacionados con el fraude electrónico.
- Los actos relacionados con la comercialización o con el tráfico de drogas por medios electrónicos.
- Los actos relacionados con el blanqueo de dinero por medios electrónicos.

México

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

Criminalización

La jurisdicción nacional será un elemento fundamental a efectos de definir las obligaciones en materia de criminalización. Al respecto, México considera que la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y la Convención de las Naciones Unidas contra la Corrupción ofrecen ejemplos de disposiciones que se aplican por extensión a la lucha contra los delitos relativos al uso de tecnologías de la información y las comunicaciones, excepto en los casos vinculados a la información en la nube, que exigirán un análisis y debate más detenidos de las experiencias que se ha adquirido recientemente como consecuencia de la realización de investigaciones concretas.

Como punto de partida para la tipificación deberían tenerse en cuenta en la Convención las conductas que ya han sido reconocidas como delitos en el derecho internacional, en particular según lo establecido en otros tratados aprobados en el marco de las Naciones Unidas, y que se llevan a cabo utilizando tecnología de la información y las comunicaciones y medios electrónicos y digitales. Por lo tanto, se recomienda incluir el siguiente artículo:

> "*Los Estados partes reconocen como delitos a los fines de la presente Convención, todos los actos delictivos reconocidos por el derecho internacional vigente que se cometan utilizando tecnologías de la información y medios electrónicos*".

Entre otros delitos, para el Gobierno de México, será fundamental incluir aquellos relacionados con la explotación sexual de menores, así como los relacionados con la violencia de género, que se cometan utilizando tecnología de la información y las comunicaciones.

Se recomienda que se incluyan elementos operativos para fortalecer las investigaciones y los enjuiciamientos; para lo cual convendría considerar la posibilidad de que se incluyan anexos con plantillas en que se especifiquen los datos que se necesitan a fin de proceder con las solicitudes de información.

Dado que no se espera que se elabore una lista de todos los tipos de delitos posibles, sino principalmente de los delitos basados en la cibernética, y a fin de evitar que existan incompatibilidades o duplicaciones de leyes nacionales, se recomienda que se incluya un compromiso general por los Estados Miembros de armonizar sus legislaciones, de ser necesario.

> "*Nada en la presente Convención afectará a los derechos, obligaciones y responsabilidades de los Estados y las personas con arreglo al derecho internacional vigente que estén orientados a prevenir y contrarrestar el uso de las tecnologías de la información y las comunicaciones con fines delictivos*".

> "*En todas las acciones dirigidas a la aplicación de la presente Convención, se tendrán en cuenta en primer lugar los intereses de las víctimas – las personas físicas y las instituciones y organizaciones – de los delitos reconocidos en la presente Convención, que constituirán la consideración principal*".

Nueva Zelandia

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

Disposiciones relativas a la criminalización

1. Durante la primera sesión, se expresó un amplio apoyo y ninguna oposición, a que se incluyeran disposiciones contra la ciberdelincuencia en la convención, en particular delitos basados en la cibernética y un rango limitado de delitos facilitados por la cibernética.

2. En el anexo I del presente documento, proponemos una lista de disposiciones relativas a la criminalización con respecto a las cuales Nueva Zelandia considera que existen las mayores probabilidades de lograr un consenso y que debería, por lo tanto, constituir el centro de la atención del Comité Especial, dadas las limitaciones de recursos y tiempo. También sugerimos algunos textos para asistir en la elaboración de esas disposiciones, que han sido tomados de otros instrumentos internacionales pertinentes, como la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, la Convención de las Naciones Unidas contra la Corrupción y el Convenio sobre la Ciberdelincuencia (Convenio de Budapest).

3. Nueva Zelandia apoya que se incluya una disposición sobre jurisdicción que refleje, cuando proceda, los instrumentos vigentes, como el artículo 42 de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, con otros elementos que obliguen a los Estados a ejercer jurisdicción cuando el delito o parte del delito se cometa en el territorio del Estado parte, para reflejar el hecho de que es posible que los delitos cibernéticos se cometan en el ciberespacio, y que el autor, la víctima, los datos y los sistemas informáticos se utilicen en distintas jurisdicciones.

Anexo 1 – Disposiciones relativas a la criminalización

Acceso ilícito a sistemas informáticos

Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a todo o parte de un sistema informático. Las Partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático.

Interceptación ilícita de datos informáticos

Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos. Las Partes podrán exigir que el delito se cometa con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

Ataque a la integridad de los datos informáticos

1. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos.

2. Las Partes podrán reservarse el derecho a exigir que los actos definidos en el párrafo 1 comporten daños graves.

Ataque a la integridad del funcionamiento de un sistema informático

Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima, del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

Uso indebido de dispositivos o programas informáticos

1. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a) la producción, venta, obtención para su utilización, importación, distribución o cualquier otra forma de puesta a disposición de:

i) cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos previstos en [artículos pertinentes];

ii) una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con intención de que sean utilizados para cometer cualquiera de los delitos previstos en [artículos pertinentes], y

b) la posesión de alguno de los elementos contemplados en los incisos i) o ii) del apartado a) del presente párrafo con intención de que sean utilizados para cometer cualquiera de los delitos previstos en [artículos pertinentes]. Las Partes podrán exigir en su derecho interno la posesión de un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

2. No se interpretará que el presente artículo impone responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, distribución o cualquier otra forma de puesta a disposición o la posesión mencionada en el párrafo 1 del presente artículo no tenga por objeto la comisión de uno de los delitos previstos de conformidad con [artículos pertinentes], como en el caso de las pruebas autorizadas o de la protección de un sistema informático.

3. Cada Parte podrá reservarse el derecho a no aplicar el párrafo 1 del presente artículo, siempre que dicha reserva no afecte a la venta, distribución o cualquier otra forma de puesta a disposición de los elementos mencionados en el inciso ii) del apartado a) del párrafo 1.

Criminalización de la ciberextorsión

1. Nueva Zelandia apoyaría que se incluyera una disposición en que se tipificara:

a) la extorsión al usuario de un sistema informático para que desbloquee datos;

b) la extorsión al usuario de un sistema informático con la amenaza de que se publicarán datos o información personal sin autorización.

2. Nueva Zelandia espera con interés cooperar con colegas para encontrar una redacción precisa para esta figura penal.

Fraude informático

Cada Parte adoptará las medidas legislativas o de otra índole que resulten necesarias para tipificar como delito en su derecho interno los actos que se cometan deliberadamente y sin tener derecho a ello que causen perjuicio patrimonial a otra persona mediante:

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

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

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

Falsificación informática

Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente. Las Partes podrán exigir que exista la intención fraudulenta, o una intención delictiva similar, para que se considere que existe responsabilidad penal.

Explotación sexual de niños mediante la utilización de sistemas informáticos

1. Esperamos con interés cooperar con nuestros colegas en la elaboración de disposiciones integrales y eficaces relativas a la represión de la explotación y abusos sexuales de niños en línea.

2. Como mínimo, esos delitos deberían incluir delitos relacionados con el uso de sistemas informáticos para:

a) producir material que muestre la explotación sexual de niños;

b) ofrecer o poner a disposición material que muestre la explotación sexual de niños;

c) distribuir o transmitir material que muestre la explotación sexual de niños;

d) adquirir, para uno mismo o para otra persona, material que muestre la explotación sexual de niños;

e) poseer material que muestre la explotación sexual de niños;

f) captar niños con fines sexuales.

Publicación o distribución de grabaciones de imágenes íntimas sin consentimiento

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito, en su derecho interno, la transferencia, envío, publicación, diseminación o comunicación, por medio de sistemas informáticos, sin contar con un motivo razonable, de una grabación de imágenes íntimas de la víctima:

a) a sabiendas de que la víctima no ha consentido la publicación; o

b) despreocupándose en forma irresponsable de que la víctima haya consentido la publicación.

2. Debería establecerse que un niño o una persona joven de menos de 16 años no puede consentir la publicación de una grabación de imágenes íntimas de sí.

Participación y tentativa

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

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

Responsabilidad de las personas jurídicas

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

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

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

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

5. Las personas jurídicas estarán exentas de responsabilidad respecto de actos que hayan sido cometidos u omitidos de buena fe:

a) al cumplir o intentar cumplir una obligación impuesta por la presente Convención o de conformidad con ella, o

b) al ejercer o intentar ejercer una función o facultad conferidas por la presente Convención o de conformidad con ella.

Tipificación del blanqueo de dinero

1. Cada Estado parte adoptará, de conformidad con los principios fundamentales de su derecho interno, las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito, cuando se cometan intencionalmente:

a) i) la conversión o la transferencia de bienes, a sabiendas de que esos bienes son producto de la ciberdelincuencia, con el propósito de ocultar o disimular el origen ilícito de los bienes o ayudar a cualquier persona involucrada en la comisión del delito determinante a eludir las consecuencias jurídicas de sus actos;

ii) la ocultación o disimulación de la verdadera naturaleza, origen, ubicación, disposición, movimiento o propiedad de bienes o derecho sobre estos, a sabiendas de que dichos bienes son producto de la ciberdelincuencia;

b) con sujeción a los conceptos básicos de su ordenamiento jurídico:

i) la adquisición, posesión o utilización de bienes, a sabiendas, en el momento de su recepción, de que son producto de la ciberdelincuencia;

ii) la participación en la comisión de cualesquiera de los delitos tipificados con arreglo al presente artículo, así como la asociación y la confabulación para cometerlos, la tentativa de cometerlos y la ayuda, la incitación, la facilitación y el asesoramiento en aras de su comisión.

2. Para los fines de la aplicación o puesta en práctica del párrafo 1 del presente artículo:

a) Cada Estado parte velará por aplicar el párrafo 1 del presente artículo a la gama más amplia posible de delitos determinantes.

b) Cada Estado parte incluirá como delitos determinantes [delitos pertinentes establecidos en el artículo pertinente de la presente Convención y] los delitos tipificados con arreglo a [los artículos pertinentes] de la presente Convención. Los Estados parte cuya legislación establezca una lista de delitos determinantes incluirán entre estos, como mínimo [una amplia gama de delitos relacionados con la ciberdelincuencia].

c) A los efectos del apartado b), los delitos determinantes incluirán los delitos cometidos tanto dentro como fuera de la jurisdicción del Estado parte interesado. No obstante, los delitos cometidos fuera de la jurisdicción de un Estado parte constituirán delito determinante siempre y cuando el acto correspondiente sea delito con arreglo al derecho interno del Estado en que se haya cometido y constituyese asimismo delito con

arreglo al derecho interno del Estado parte que aplique o ponga en práctica el presente artículo si el delito se hubiese cometido allí.

d) Cada Estado parte proporcionará al Secretario General de las Naciones Unidas una copia de sus leyes destinadas a dar aplicación al presente artículo y de cualquier enmienda ulterior que se haga a tales leyes o una descripción de esta.

e) Si así lo requieren los principios fundamentales del derecho interno de un Estado parte, podrá disponerse que los delitos tipificados en el párrafo 1 del presente artículo no se aplicarán a las personas que hayan cometido el delito determinante.

f) El conocimiento, la intención o la finalidad que se requieren como elemento de un delito tipificado en el párrafo 1 del presente artículo podrán inferirse de circunstancias fácticas objetivas.

Obstrucción de la justicia

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito, cuando se cometan intencionalmente:

a) El uso de fuerza física, amenazas o intimidación, o la promesa, el ofrecimiento o la concesión de un beneficio indebido para inducir a falso testimonio u obstaculizar la prestación de testimonio o la aportación de pruebas en un proceso en relación con la comisión de uno de los delitos comprendidos en la presente Convención.

b) El uso de fuerza física, amenazas o intimidación para obstaculizar el cumplimiento de las funciones oficiales de un funcionario de la justicia o de los servicios encargados de hacer cumplir la ley en relación con la comisión de los delitos comprendidos en la presente Convención. Nada de lo previsto en el presente apartado menoscabará el derecho de los Estados parte a disponer de legislación que proteja a otras categorías de funcionarios públicos.

Noruega

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

Criminalización

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

- el acceso ilícito, es decir, el acto de acceder a una computadora o sistema informático sin autorización;
- la interceptación ilícita, es decir, la interceptación contraria a derecho en tiempo real del contenido de las comunicaciones o de los datos de tráfico relacionados con las comunicaciones;
- el ataque a la integridad de los datos o sistemas, es decir, el uso de programas maliciosos, los ataques de denegación de servicio, el uso de programas secuestradores y la eliminación o modificación de datos;
- el uso abusivo de dispositivos, es decir, el tráfico o la utilización de datos de crédito, contraseñas e información personal que den acceso a los recursos.

2. Nos parece conveniente que la lista sea breve.

3. En la convención también debería evitarse la duplicación de delitos previstos en otros instrumentos jurídicos.

4. El texto debería ser neutro desde el punto de vista tecnológico.

5. Además de una lista breve de delitos basados en la cibernética, en la convención deberían incluirse disposiciones sobre delitos en que se utilice material que muestre abusos sexuales de niños.

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

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

Capítulo II
Tipificación, procedimiento penal y aplicación de la ley

Sección 1
Atribución de responsabilidad

Artículo 5
Atribución de responsabilidad

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su legislación interna, como mínimo, las conductas enunciadas en los artículos 6, 7, 9 a 12, 14 a 17, 19, 20, 22 a 26 y 28 de la presente Convención, aplicando para ello las sanciones penales y de otra índole, incluida la pena de prisión, que correspondan a la peligrosidad del acto concreto y la cuantía del daño causado.

Artículo 6
Acceso ilícito a la información digital

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su legislación interna el acceso ilícito y deliberado a información digital que tenga como resultado que dicha información se destruya, se bloquee, se modifique o se copie.

Artículo 7
Interceptación ilícita

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su legislación interna la interceptación deliberada de información digital, realizada sin la autorización correspondiente, o en violación de las normas establecidas, incluida la utilización de medios técnicos de interceptación de parámetros técnicos del tráfico y de datos procesados mediante tecnologías de la información y las comunicaciones y no destinados a su utilización pública.

Artículo 8
Interferencia ilícita en la información digital

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito u otro acto ilícito en su legislación interna la destrucción, la eliminación, la alteración, el bloqueo, la modificación o el copiado deliberados de información digital.

Artículo 9
Perturbación de las redes de información y comunicaciones

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su legislación interna todo acto ilícito y deliberado destinado a perturbar el funcionamiento de las redes de información y comunicaciones que produzca o amenace con producir graves consecuencias.

Artículo 10
Creación, utilización y distribución de programas maliciosos

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su legislación interna la creación, adaptación, utilización y distribución deliberadas de programas maliciosos destinados a la destrucción, el bloqueo, la modificación, el copiado o la difusión de información digital o la neutralización de sus funciones de seguridad sin autorización, excepto en el marco de investigaciones legítimas.

2. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito u otro acto ilícito en su legislación interna la creación o utilización de redes de bots con el fin de cometer cualquiera de los actos enunciados en los artículos 6 a 12 y 14 de la presente Convención.

Artículo 11
Interferencia ilícita en infraestructuras de información críticas

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su legislación interna la creación, distribución o utilización deliberadas de programas informáticos u otra información digital diseñados con la intención de interferir ilícitamente en infraestructuras de información críticas, incluidos los programas informáticos u otra información digital para destruir, bloquear, modificar y copiar la información contenida en ellos o para neutralizar las funciones de seguridad.

2. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su legislación interna la infracción de las normas de funcionamiento de los medios diseñados para almacenar, procesar o transferir la información digital protegida contenida en infraestructuras de información críticas o los sistemas de información o las redes de información y comunicaciones pertenecientes a la infraestructura de información crítica, o la infracción de las normas de acceso a ellos, si esa infracción causa daños a la infraestructura de información crítica.

Artículo 12
Acceso no autorizado a datos personales

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su legislación interna el acceso no autorizado a los datos personales con el fin de destruirlos, modificarlos, copiarlos o difundirlos.

Artículo 13
Tráfico ilícito de dispositivos

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito u otro acto ilícito de conformidad con su legislación interna la fabricación, venta, compra para la utilización, importación o exportación ilícitas de dispositivos diseñados o adaptados principalmente para cometer cualquiera de los delitos enunciados en los artículos 6 a 12 de la presente Convención, u otras formas ilícitas de transferencia para la utilización de esos dispositivos.

Las disposiciones del presente artículo no se aplicarán cuando la fabricación, venta, compra para la utilización, importación, exportación u otras formas de transferencia para la utilización de dispositivos estén relacionadas, por ejemplo, con la realización de pruebas autorizadas o la protección de sistemas informáticos.

Artículo 14
Robo mediante la utilización de las tecnologías de la información y las comunicaciones

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su legislación interna el robo de bienes o la adquisición ilícita de derechos sobre ellos, incluso mediante fraude, destruyendo,

bloqueando, modificando o copiando información digital o interfiriendo de otro modo en el funcionamiento de las tecnologías de la información y las comunicaciones.

2. Cada Estado parte podrá reservarse el derecho a tratar el robo de bienes cometido mediante la tecnología de la información y las comunicaciones o la adquisición ilícita de derechos sobre ellos, incluso mediante fraude, como una circunstancia agravante en la comisión del robo, cuando este se cometa en alguna de las formas definidas en su legislación interna.

Artículo 15
Delitos relacionados con la producción y distribución de material u objetos con representaciones pornográficas de menores, cometidos mediante la utilización de las tecnologías de la información y las comunicaciones

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su legislación interna, cuando se cometan deliberada e ilícitamente, los siguientes actos:

a) la producción de pornografía infantil para su distribución a través de las redes de información y comunicaciones, en particular vía Internet;

b) la oferta o facilitación de pornografía infantil a través de las redes de información y comunicaciones, en particular vía Internet;

c) la distribución, transmisión, exhibición pública o promoción de pornografía infantil a través de las redes de información y comunicaciones, en particular vía Internet;

d) la adquisición de pornografía infantil mediante la utilización de las tecnologías de la información y las comunicaciones para uno mismo o para otra persona;

e) la posesión de pornografía infantil en un sistema informático o en un soporte digital electrónico.

2. A los efectos del párrafo 1 del presente artículo, por “pornografía infantil” se entenderá todo material pornográfico que represente:

a) la participación de menores en actos sexuales explícitos;

b) la participación de personas que parezcan ser menores en actos sexuales explícitos;

c) imágenes realistas de la participación de menores en actos sexuales explícitos.

A los efectos del presente artículo, se entenderá por “menor” toda persona menor de 18 años. Las Partes podrán, no obstante, exigir un límite de edad inferior, que deberá ser como mínimo de 16 años.

Artículo 16
Incitación o coacción al suicidio

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su legislación interna la incitación o la coacción al suicidio, incluso de menores, cometidas mediante presión psicológica o de otro tipo a través de las redes de información y comunicaciones, en particular vía Internet.

Artículo 17
Delitos relacionados con la participación de menores en la comisión de actos ilícitos peligrosos para su vida o su salud

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su legislación interna la utilización de las tecnologías de la información y las comunicaciones para hacer participar a menores en la comisión de actos ilícitos que pongan en peligro su vida, siempre que sean distintos de los previstos en el artículo 16 de la presente Convención.

Artículo18
Creación y utilización de información digital para engañar al usuario

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito u otro acto ilícito en su legislación interna la creación y utilización ilícitas y deliberadas de información digital que pueda confundirse con información ya conocida y considerada fiable por el usuario, de modo que se cause un daño sustancial.

2. Cada Estado parte podrá reservarse el derecho a considerar tales actos como criminales si se cometen junto con otros delitos previstos en la legislación interna del Estado parte o si se albergaba la intención deliberada de cometerlos.

Artículo 19
Incitación a cometer actos subversivos o armados

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su legislación interna toda exhortación, mediante la utilización de las tecnologías de la información y las comunicaciones, a cometer actos subversivos o armados que tengan por objeto el derrocamiento por la violencia del Gobierno de otro Estado.

Artículo 20
Delitos relacionados con actividades terroristas

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su legislación interna toda exhortación, emitida mediante la utilización de las tecnologías de la información y las comunicaciones, a la realización de actividades terroristas, la inducción, el reclutamiento u otra forma de participación en actividades terroristas, la propaganda y la justificación del terrorismo o la recaudación o el suministro de fondos para su financiación.

Artículo 21
Delitos relacionados con actividades extremistas

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito u otro acto ilícito en su legislación interna la distribución de material que exhorte a la comisión de actos ilícitos motivados por el odio o la enemistad política, ideológica, social, racial, étnica o religiosa; la promoción y la justificación de esos actos o la facilitación de acceso a ese material, realizadas mediante la utilización de las tecnologías de la información y las comunicaciones.

2. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito u otro acto ilícito en su legislación interna la humillación, mediante la utilización de las tecnologías de la información y las comunicaciones, de una persona o un grupo de personas en razón de su raza, etnia, idioma, origen o afiliación religiosa.

Artículo 22
Delitos relacionados con la distribución de estupefacientes y sustancias psicotrópicas

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su legislación interna el tráfico deliberado de estupefacientes y sustancias psicotrópicas y del material necesario para su fabricación mediante la utilización de las tecnologías de la información y las comunicaciones.

Artículo 23
Delitos relacionados con el tráfico ilícito de armas

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su legislación interna el tráfico ilícito y deliberado de armas, municiones, artefactos explosivos y sustancias explosivas, mediante la utilización de las tecnologías de la información y las comunicaciones.

Artículo 24
Rehabilitación del nazismo y justificación del genocidio o de los crímenes contra la paz y crímenes de lesa humanidad

Cada Estado adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su legislación interna la difusión deliberada, mediante la utilización de las tecnologías de la información y las comunicaciones, de material que niegue, apruebe o justifique actos que constituyan genocidio o crímenes contra la paz y crímenes de lesa humanidad, de conformidad con la sentencia del Tribunal Militar Internacional establecido en virtud del Acuerdo de Londres de 8 de agosto de 1945.

Artículo 25
Distribución ilícita de medicamentos y productos médicos falsificados

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su legislación interna la distribución ilícita y deliberada de medicamentos y productos médicos falsificados mediante tecnologías de la información y las comunicaciones.

Artículo 26
Utilización de las tecnologías de la información y las comunicaciones para cometer actos definidos como crímenes en el derecho internacional

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su legislación interna la utilización de las tecnologías de la información y las comunicaciones para cometer un acto que constituya un delito contemplado en cualquiera de los instrumentos internacionales enumerados en el Anexo[36] de la presente Convención.

2. Al depositar su instrumento de ratificación, aceptación, aprobación o adhesión, todo Estado que no sea parte en ninguno de los instrumentos enumerados en el Anexo de la presente Convención podrá declarar que, en lo concerniente a la aplicación de la presente Convención a ese Estado parte, el instrumento de que se trate se considerará no incluido en dicho Anexo. La declaración dejará de tener efecto tan pronto como el instrumento entre en vigor para ese Estado parte, que notificará al depositario de esa circunstancia.

3. Cuando un Estado parte deje de ser parte en un instrumento enumerado en el Anexo de la presente Convención, podrá hacer una declaración con respecto al instrumento o los instrumentos de que se trate, según lo previsto en el párrafo 2 del presente artículo.

Artículo 27
Infracción de los derechos de autor y derechos afines mediante la utilización de las tecnologías de la información y las comunicaciones

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito u otro acto ilícito en su legislación interna la infracción de los derechos de autor y derechos afines, según se encuentren definidos en la legislación de ese Estado parte, cuando se cometa deliberadamente mediante la utilización de tecnologías de la información y las comunicaciones, incluida la utilización ilícita de programas para sistemas informáticos o bases de datos sujetos a derechos de autor y la atribución a sí mismo de la autoría de una obra.

[36] Nota de la Secretaría: véase el documento A/75/980.

Artículo 28
Complicidad en la comisión de un delito, preparación de la comisión de un delito y tentativa de comisión de un delito

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su legislación interna la preparación y la tentativa de comisión de un delito tipificado con arreglo a la presente Convención.

2. Cada Estado parte considerará la posibilidad de adoptar las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su legislación interna la fabricación o adaptación por una persona de instrumentos u otros medios para cometer un delito, el reclutamiento de cómplices, la conspiración para cometer un delito o cualquier otra forma de creación deliberada de condiciones por una persona para cometer un delito tipificado con arreglo a la presente Convención, cuando el delito no se haya cometido en virtud de circunstancias ajenas a la voluntad de esa persona.

3. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias de conformidad con su legislación interna para establecer la responsabilidad, no solo de los autores materiales de un delito tipificado con arreglo a la presente Convención, sino también de los organizadores, instigadores o cómplices involucrados, así como para agravar la responsabilidad por los delitos cometidos en grupo, tales como los cometidos por grupos organizados y asociaciones delictivas.

Artículo 29
Otros actos ilícitos

La presente Convención no habrá de ser obstáculo para que un Estado parte tipifique como delito cualquier otro acto ilícito cometido deliberadamente mediante la utilización de las tecnologías de la información y las comunicaciones que cause un daño sustancial.

Artículo 30
Responsabilidad de las personas jurídicas

1. Cada Estado parte adoptará las medidas legislativas y otras medidas jurídicas que resulten necesarias para que las personas jurídicas puedan ser consideradas responsables de los delitos y otros actos ilícitos tipificados con arreglo a la presente Convención, cuando sean cometidos en su provecho por cualquier persona física que actúe a título individual o como miembro de un órgano de la persona jurídica de que se trate y que ocupe un cargo directivo en esa persona jurídica en virtud de lo siguiente:

a) la autorización para representar a la persona jurídica en cuestión;

b) el derecho a adoptar decisiones en nombre de esa persona jurídica;

c) el derecho a ejercer el control en el seno de esa persona jurídica.

2. Además de los casos contemplados en el párrafo 1 del presente artículo, cada Estado parte adoptará las medidas necesarias para que pueda exigirse responsabilidad a una persona jurídica cuando la falta de supervisión o control por la persona física mencionada en el párrafo 1 haga posible que una persona física que actúe bajo su autoridad cometa en beneficio de esa persona jurídica un delito u otro acto ilícito tipificado con arreglo a la presente Convención.

3. Con sujeción a los principios jurídicos de cada Estado parte, la responsabilidad de una persona jurídica puede ser penal, civil o administrativa. Cada Estado parte se asegurará de que las personas jurídicas consideradas responsables sean objeto de sanciones efectivas, proporcionales y disuasorias, incluidas sanciones financieras.

4. La responsabilidad de las personas jurídicas no excluye la responsabilidad de las personas físicas que hayan cometido un delito u otro acto ilícito.

Sudáfrica

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

Capítulo II. Criminalización

Artículo 5: Acceso ilícito

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno el acceso ilícito, deliberado e ilegítimo a todo o parte de un sistema informático. Las Partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos ilícitamente o con alguna otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático.

Artículo 6: Interceptación ilícita

Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos. Las Partes podrán exigir que el delito se cometa con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

Artículo 7: Interferencia no autorizada con información digital

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos.

2. Las Partes podrán reservarse el derecho a exigir que la conducta descrita en el párrafo 1 tenga como consecuencia la producción de un daño grave (a personas físicas, personas jurídicas y la economía de un Estado parte).

Artículo 8: Ataques a la integridad del sistema y perturbación de redes de información y comunicaciones

Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima, del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

Artículo 9: Creación, utilización y distribución de dispositivos

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno, cuando se los cometa deliberada e ilegítimamente, los siguientes actos:

a) la producción, venta, obtención para su utilización, importación, distribución o cualquier otra forma de puesta a disposición de:

i) cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos previstos en los artículos 5 a 26;

ii) una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con intención de que sean utilizados para cometer cualquiera de los delitos contemplados en los artículos 5 a 26, y

b) la posesión de alguno de los elementos contemplados en los incisos i) o ii) del apartado a) del presente párrafo con intención de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 5 a 26. Las Partes podrán exigir en su derecho interno la posesión de un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

2. No se interpretará que el presente artículo impone responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, distribución o cualquier otra forma de puesta a disposición o la posesión mencionada en el párrafo 1 del presente artículo no tenga por objeto la comisión de uno de los delitos previstos de conformidad con los artículos 5 a 26 de la presente Convención, como en el caso de las pruebas autorizadas o de la protección de un sistema informático.

3. Los Estados partes podrán reservarse el derecho a no aplicar el párrafo 1 del presente artículo, siempre que dicha reserva no afecte a la venta, distribución o cualquier otra forma de puesta a disposición de los elementos mencionados en el inciso ii) del apartado a) del párrafo 1.

Artículo 10: Falsificación facilitada por la cibernética

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la introducción, alteración, borrado o supresión deliberadas e ilegítimas de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente. Las Partes podrán exigir que exista una intención fraudulenta o delictiva similar para que se considere que existe responsabilidad penal.

Artículo 11: Fraude facilitado por la cibernética

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno el causar perjuicio patrimonial, deliberada, ilícita e ilegítimamente, a otra persona mediante:

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

b) cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva, de obtener, sin tener derecho a ello, un beneficio económico para uno mismo o para otra persona.

Artículo 12: Delitos en que se utilice material que muestre abusos sexuales de niños

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a) la producción de material que muestre abusos sexuales de niños a fines de su distribución mediante sistemas informáticos o tecnología de la información y las comunicaciones;

b) el ofrecimiento o puesta a disposición de material que muestre abusos sexuales de niños mediante sistemas informáticos o tecnología de la información y las comunicaciones;

c) la distribución o transmisión de material que muestre abusos sexuales de niños mediante sistemas informáticos o tecnología de la información y las comunicaciones;

d) la obtención de material que muestre abusos sexuales de niños mediante sistemas informáticos o tecnología de la información y las comunicaciones para uno mismo o para otra persona;

e) la posesión de material que muestre abusos sexuales de niños en un sistema informático o de tecnología de la información y las comunicaciones o en un medio de almacenamientos de datos informáticos.

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

a) un menor adoptando un comportamiento sexualmente explícito;

b) una persona que parezca un menor adoptando un comportamiento sexualmente explícito, y

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

3. A los efectos del párrafo 2 anterior, se entenderá por “menor” toda persona menor de 18 años. Las Partes podrán, no obstante, exigir un límite de edad inferior, que deberá ser como mínimo de 16 años.

Artículo 13: Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno las infracciones de la propiedad intelectual que defina su legislación, de conformidad con las obligaciones que haya contraído en aplicación de los distintos convenios y acuerdos internacionales, a excepción de cualquier derecho moral otorgado por dichos tratados, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático o de tecnología de la información y las comunicaciones.

2. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno las infracciones de los derechos afines definidas en su legislación, de conformidad con las obligaciones que haya asumido en aplicación de la Convención Internacional para la Protección de los Artistas, Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodistribución (Convención de Roma), del Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual Relacionados con el Comercio y del Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas, a excepción de cualquier derecho moral conferido por dichos tratados, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático o de tecnología de la información y las comunicaciones.

3. Un Estado parte podrá reservarse el derecho de no imponer responsabilidad penal en virtud de los párrafos 1 y 2 del presente artículo en limitadas circunstancias, siempre que se disponga de otros recursos efectivos y que dicha reserva no vulnere las obligaciones internacionales que incumban a dicha Parte en aplicación de los instrumentos internacionales mencionados en los párrafos 1 y 2 del presente artículo.

Artículo 14: Delitos relacionados con la distribución ilícita de estupefacientes y sustancias sicotrópicas

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno actos relacionados con el uso de las tecnologías de la información y las comunicaciones, que promuevan el tráfico de estupefacientes, sustancias sicotrópicas y material que sea necesario para su fabricación.

Artículo 15: Protección de los denunciantes

Cada Estado parte considerará la posibilidad de incorporar en su ordenamiento jurídico interno medidas apropiadas para proporcionar protección contra todo trato injustificado a las personas que denuncien ante las autoridades competentes, de buena fe y con motivos razonables, cualesquiera hechos concernientes a delitos relacionados con el uso de las tecnologías de la información y las comunicaciones tipificados con arreglo a la presente Convención.

Cada Estado parte considerará la posibilidad de establecer en su ordenamiento jurídico protección contra el enjuiciamiento, con sujeción al cumplimiento de las normas y condiciones aprobadas por la Parte, de cualquiera que preste plena

cooperación y de buena fe cuando interactúe con las autoridades encargadas de hacer cumplir la ley.

Artículo 16: Cooperación con las autoridades encargadas de hacer cumplir la ley

1. Cada Estado parte adoptará medidas apropiadas para alentar a las personas que participen o hayan participado en la comisión de delitos tipificados con arreglo a la presente Convención relacionados con el uso de las tecnologías de la información y las comunicaciones a que proporcionen a las autoridades competentes de buena fe información útil con fines investigativos y probatorios y a que les presten ayuda efectiva y concreta que pueda contribuir a privar a los delincuentes del producto del delito, así como a recuperar ese producto.

2. Cada Estado parte considerará la posibilidad de prever, en casos apropiados, la mitigación de la pena de toda persona acusada que preste de buena fe cooperación sustancial en la investigación y el enjuiciamiento de los delitos relacionados con el uso de las tecnologías de la información y las comunicaciones tipificados con arreglo a la presente Convención.

3. Cada Estado parte considerará la posibilidad de prever, de conformidad con los principios fundamentales de su derecho interno, la concesión de inmunidad judicial a toda persona que, de buena fe, preste cooperación sustancial en la investigación o el enjuiciamiento de los delitos relativos al uso de las tecnologías de la información y las comunicaciones tipificados con arreglo a la presente Convención.

4. La protección de esas personas será, *mutatis mutandis*, la prevista en el artículo 22 de la presente Convención.

5. Cuando las personas mencionadas en el párrafo 1 del presente artículo se encuentren en un Estado parte y puedan prestar cooperación sustancial a las autoridades competentes de otro Estado parte, los Estados partes interesados podrán considerar la posibilidad de celebrar acuerdos o arreglos, de conformidad con su derecho interno, con respecto a la eventual concesión, por el otro Estado parte, del trato previsto en los párrafos 2 y 3 del presente artículo.

6. Cada Estado parte llevará un registro que contenga información identificable de todos los registradores de nombres de dominio, los criptoactivos y los operadores de criptoactivos en su jurisdicción, de conformidad con los principios fundamentales de su derecho interno, y proporcionar esa información a las autoridades competentes con fines investigativos y probatorios.

Artículo 17: Jurisdicción

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

a) el delito se cometa en su territorio; o

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

2. Con sujeción a lo dispuesto en el artículo 4 de la presente Convención, un Estado parte también podrá establecer su jurisdicción para conocer de tales delitos relacionados con el uso de las tecnologías de la información y las comunicaciones cuando:

a) el delito se cometa contra uno de sus nacionales; o

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

c) el delito sea uno de los delitos tipificados con arreglo al apartado b) ii) del párrafo 1 del artículo 17 de la presente Convención y se cometa fuera de su territorio con miras a la comisión, dentro de su territorio, de un delito relacionado con el uso de

las tecnologías de la información y las comunicaciones tipificado con arreglo al artículo 15 de la presente Convención, o

d) El delito se cometa contra el Estado parte, o tenga repercusiones directas en los asuntos de ese Estado parte.

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

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

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

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

Suiza

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

2.2 Disposiciones relativas a la criminalización

a. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

Acceso ilícito

Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a todo o parte de un sistema informático. Las Partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático.

Interceptación ilícita

Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos. Las Partes podrán exigir que el delito se cometa con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

Ataques a la integridad de los datos informáticos

1. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos.

2. Las Partes podrán reservarse el derecho a exigir que los actos definidos en el párrafo 1 comporten daños graves.

Ataque a la integridad del sistema

Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

Uso indebido de dispositivos

1. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a) la producción, venta, obtención para su utilización, importación, distribución o cualquier otra forma de puesta a disposición de:

i) un dispositivo, incluido un programa informático, diseñado o adaptado principalmente con el fin de cometer cualquiera de los delitos tipificados con arreglo a las disposiciones de la presente Convención sobre el acceso ilícito, la interceptación ilícita o el ataque a la integridad de los datos o sistemas;

ii) una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con intención de que sean utilizados para cometer cualquiera de los delitos contemplados en las disposiciones de la presente Convención relativas al acceso o interceptación ilícitos o el ataque a la integridad de los datos o sistemas, y

b) la posesión de un elemento de los enunciados en los incisos i) o ii) del apartado a) del presente párrafo con la intención de que se utilice para cometer cualquiera de los delitos tipificados con arreglo a las disposiciones de la presente Convención relativas al acceso o interceptación ilícitos o el ataque a la integridad de los datos o sistemas. Las Partes podrán exigir la posesión de un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

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

3. Cada Parte podrá reservarse el derecho a no aplicar el párrafo 1 del presente artículo, siempre que dicha reserva no afecte a la venta, distribución o cualquier otra forma de puesta a disposición de los elementos mencionados en el inciso ii) del apartado a) del párrafo 1.

b. Delitos informáticos

Falsificación informática

Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como

auténticos, con independencia de que los datos sean legibles e inteligibles directamente. Las Partes podrán exigir que exista una intención fraudulenta o delictiva similar para que se considere que existe responsabilidad penal.

Fraude informático

Cada Parte adoptará las medidas legislativas o de otra índole que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante:

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

b) cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.

c. Delitos relacionados con el contenido

Delitos relacionados con material en que se muestre explotación y abusos sexuales de niños

1. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a) la producción de imágenes de explotación y abusos sexuales de niños con la intención de difundirla a través de un sistema informático;

b) la oferta o la puesta a disposición de material que muestre explotación y abusos sexuales a través de un sistema informático;

c) la distribución o la transmisión de material que muestre explotación y abusos sexuales de niños a través de un sistema informático;

d) la obtención, para uno mismo o para otra persona, de material que muestre explotación y abusos sexuales de niños a través de un sistema informático;

e) la posesión de material que muestre explotación y abusos sexuales de niños en un sistema informático o en un dispositivo de almacenamiento de datos informáticos.

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

a) un menor adoptando un comportamiento sexualmente explícito;

b) una persona que parezca un menor adoptando un comportamiento sexualmente explícito;

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

3. A los efectos del párrafo 2 anterior, se entenderá por “menor” toda persona menor de 18 años. Las Partes podrán, no obstante, exigir un límite de edad inferior, que deberá ser como mínimo de 16 años.

4. Cada Parte podrá reservarse el derecho a no aplicar, en todo o en parte, los apartados d) y e) del párrafo 1 y los apartados b) y c) del párrafo 2.

d. Otras formas de responsabilidad y de sanción

Tentativa y complicidad

1. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno cualquier complicidad deliberada con vistas a la comisión de alguno de los delitos previstos en las disposiciones relativas a la criminalización de la presente Convención, con la intención de que dicho delito sea cometido.

2. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno toda tentativa deliberada de cometer alguno de los delitos tipificados en las disposiciones sobre criminalización de la presente Convención.

3. Cada Parte podrá reservarse el derecho a no aplicar, en todo o en parte, el párrafo 2 del presente artículo.

Responsabilidad de las personas jurídicas

1. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para que pueda exigirse responsabilidad a una persona jurídica por los delitos tipificados con arreglo a las disposiciones de la presente Convención, cuando sean cometidos por cuenta de esta por una persona física, ya sea a título individual o como miembro de un órgano de dicha persona jurídica, que ejerza funciones directivas en su seno, en virtud de:

a) un poder de representación de la persona jurídica;

b) una autorización para tomar decisiones en nombre de la persona jurídica;

c) una autorización para ejercer funciones de control en el seno de la persona jurídica.

2. Además de los casos previstos en el párrafo 1 del presente artículo, cada Parte adoptará las medidas necesarias para garantizar que pueda exigirse responsabilidad a una persona jurídica cuando la ausencia de vigilancia o de control por parte de cualquier persona física mencionada en el párrafo 1 haya permitido la comisión de un delito previsto en aplicación de la presente Convención por una persona física por cuenta de dicha persona jurídica y bajo su autoridad.

3. Dependiendo de los principios jurídicos de la Parte, la responsabilidad de una persona jurídica podrá ser penal, civil o administrativa.

4. Dicha responsabilidad se entenderá sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido el delito.

Sanciones y medidas

1. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para que los delitos tipificados en las disposiciones relativas a la criminalización de la presente Convención estén sujetos a sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad.

2. Cada Parte garantizará la imposición de sanciones o medidas penales o no penales efectivas, proporcionadas y disuasorias, incluidas sanciones pecuniarias, a las personas jurídicas consideradas responsables de conformidad con las disposiciones sobre la responsabilidad de las personas jurídicas de la presente Convención.

Reino Unido de Gran Bretaña e Irlanda del Norte

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

Capítulo – Criminalización

Delitos basados en la cibernética

El Reino Unido considera que la convención debe incluir los delitos basados en la cibernética y contener descripciones y definiciones que sean aceptables para todas las partes, y que guarden coherencia con los acuerdos internacionales vigentes en esa esfera.

Artículo 5
Acceso ilícito

Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a todo o parte de un sistema informático. Las Partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático.

Artículo 6
Interceptación ilícita

Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos. Las Partes podrán exigir que el delito se cometa con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

Artículo 7
Ataques a la integridad de los datos

1. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos.

2. Las Partes podrán reservarse el derecho a exigir que los actos definidos en el párrafo 1 comporten daños graves.

Artículo 8
Ataques a la integridad del sistema

Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

Artículo 9
Uso indebido de los dispositivos

1. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a) la producción, venta, obtención para su utilización, importación, distribución o cualquier otra forma de puesta a disposición de:

i) cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos tipificados con arreglo a las secciones;

ii) una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con intención de que sean utilizados para cometer cualquiera de los delitos contemplados en los otro cuatro artículos que figuran en la presente sección, y

b) la posesión de alguno de los elementos contemplados en los incisos i) o ii) del apartado a) del presente párrafo con intención de que sean utilizados para cometer cualquiera de los delitos previstos en los otro cuatro artículos que figuran en la presente sección. Las Partes podrán exigir en su derecho interno la posesión de un número

determinado de dichos elementos para que se considere que existe responsabilidad penal.

2. No se interpretará que el presente artículo impone responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, distribución o cualquier otra forma de puesta a disposición o la posesión mencionada en el párrafo 1 del presente artículo no tenga por objeto la comisión de uno de los delitos previstos de conformidad con los artículos sobre el acceso o la interpretación ilícitos, el ataque a la integridad de los datos y sistemas, como en el caso de las pruebas autorizadas o de la protección de un sistema informático.

3. Las Partes podrán reservarse el derecho a no aplicar el párrafo 1 del presente artículo, siempre que dicha reserva no afecte a la venta, distribución o cualquier otra forma de puesta a disposición de los elementos mencionados en el inciso ii) del apartado a) del párrafo 1.

Delitos facilitados por la cibernética

El Reino Unido también considera que los delitos facilitados por la cibernética deberían incluirse si el delito se comete principalmente en línea, si el uso de computadoras modifica la escala en que se comete y la rapidez con que se perpetra y si la definición del delito se entiende comúnmente.

Artículo 10
Fraude

Cada Parte hará las reformas legislativas y adoptará las otras medidas que resulten necesarias para tipificar como delito en su derecho interno una figura básica de fraude cometido total o parcialmente en línea. Ello incluirá, pero no se limitará, a las actividades que se realicen en el país y a través de las fronteras por Internet u otros medios digitales o basados en la cibernética, con los siguientes métodos:

a) fraude cometido mediante una representación engañosa;

b) fraude cometido mediante el hecho de no revelar información;

c) el fraude cometido mediante el uso abusivo de una posición, con la intención fraudulenta o delictiva de causar un perjuicio a un tercero u obtener dinero u otros bienes para otra persona.

Artículo 11
Delitos relacionados con la explotación y los abusos sexuales de niños en línea, incluido el material que muestre explotación y abusos sexuales de niños y la captación de niños por Internet con fines sexuales

1. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a) la producción de material que muestre explotación y abusos sexuales de niños con la intención de distribuirla a través de un sistema informático;

b) la oferta o la puesta a disposición de material que muestre explotación y abusos sexuales de niños a través de un sistema informático;

c) la distribución o la transmisión de material que muestre explotación y abusos sexuales de niños a través de un sistema informático;

d) la obtención, para uno mismo o para otra persona, de material que muestre explotación y abusos sexuales de niños a través de un sistema informático;

e) la posesión de material que muestre explotación y abusos sexuales de niños en un sistema informático o en un dispositivo de almacenamiento de datos informáticos;

f) la acción de mirar material que muestre explotación y abusos sexuales de niños en un dispositivo de almacenamiento de datos informáticos.

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

a) un menor adoptando un comportamiento sexualmente explícito, real o simulado;

b) una persona que parezca un menor adoptando un comportamiento sexualmente explícito, real o simulado;

c) imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito, real o simulado;

d) cualquier representación de los órganos sexuales de un menor con fines principalmente sexuales.

3. A los efectos del párrafo 2 anterior, se entenderá por “menor” toda persona menor de 18 años. Las Partes podrán, no obstante, exigir un límite de edad inferior, que deberá ser como mínimo de 16 años.

4. Cada Parte podrá reservarse el derecho a no aplicar, en todo o en parte, los apartados d) y e) del párrafo 1 y los apartados b) y c) del párrafo 2.

Artículo 12
Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

1. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno las infracciones de la propiedad intelectual que defina su legislación, de conformidad con las obligaciones que haya contraído en aplicación del Acta de París de 24 de julio de 1971, por la cual se revisó el Convenio de Berna para la protección de las obras literarias y artísticas, del Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual Relacionados con el Comercio y del Tratado de la Organización Mundial de la Propiedad Intelectual (OMPI) sobre Derecho de Autor, a excepción de cualquier derecho moral otorgado por dichos tratados, cuando tales actos se cometan intencionalmente, a escala comercial y por medio de un sistema informático.

2. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno las infracciones de los derechos afines definidas en su legislación, de conformidad con las obligaciones que haya asumido en aplicación de la Convención Internacional sobre la Protección de los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodistribución (Convención de Roma), del Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual Relacionados con el Comercio y del Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas, a excepción de cualquier derecho moral conferido por dichos tratados, cuando tales actos se cometan intencionalmente, a escala comercial y por medio de un sistema informático.

3. Las Partes podrán reservarse el derecho de no imponer responsabilidad penal en virtud de los párrafos 1 y 2 del presente artículo en circunstancias limitadas, siempre que se disponga de otros recursos efectivos y que dicha reserva no vulnere las obligaciones internacionales que incumban a dicha Parte en aplicación de los instrumentos internacionales mencionados en los párrafos 1 y 2 del presente artículo.

Artículo 13
Tentativa y complicidad

1. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno cualquier complicidad deliberada con vistas a la comisión de alguno de los delitos tipificados con arreglo a [la presente Convención], con la intención de que dicho delito sea cometido.

2. Cada Parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno toda tentativa deliberada de cometer alguno de los delitos tipificados con arreglo a la presente Convención.

3. Cada Parte podrá reservarse el derecho a no aplicar, en todo o en parte, el párrafo 2 del presente artículo.

Artículo 14
Proceso, fallo y sanciones

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

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

3. Cuando se trate de delitos tipificados con arreglo a la presente Convención, cada Parte adoptará medidas apropiadas, de conformidad con su derecho interno y tomando debidamente en consideración los derechos de la defensa, con miras a procurar que, al imponer condiciones en relación con la decisión de conceder la libertad en espera de juicio o la apelación, se tenga presente la necesidad de garantizar la comparecencia del acusado en todo procedimiento penal ulterior.

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

5. Cada Parte establecerá, cuando proceda, con arreglo a su derecho interno, un plazo de prescripción prolongado dentro del cual pueda iniciarse el proceso por cualquiera de los delitos comprendidos en la presente Convención y un plazo mayor cuando el presunto delincuente haya eludido la administración de justicia.

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

Artículo 15
Jurisdicción

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

a) el delito se cometa en su territorio, o

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

2. Con sujeción a lo dispuesto en los artículos pertinentes de la presente Convención, las Partes también podrán establecer su jurisdicción para conocer de tales delitos cuando:

a) el delito se cometa contra uno de sus nacionales; o

b) el delito sea cometido por uno de sus nacionales o por una persona apátrida que tenga residencia habitual en su territorio, o

c) el delito se cometa contra la Parte.

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

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

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

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

Otras observaciones

El Reino Unido considera que debe penalizarse el uso de la tecnología digital para comunicarse con un menor cuando esa comunicación sea de índole sexual o se realice con la intención de alentar al menor a ser parte en una comunicación sexual o realizar una actividad sexual y cuando esa comunicación se haga con la finalidad de obtener gratificación sexual. Proporcionaremos un texto sobre esta cuestión durante las negociaciones.

El tráfico y la explotación sexuales de mujeres y niñas constituye un delito que causa un daño especialmente grave y las víctimas son objeto de una multiplicidad de abusos mientras dura su explotación que provoca un daño emocional y físico muy elevado. Dado que gran parte de esa explotación se arregla y se facilita en línea, se trata de una cuestión mundial, y el Reino Unido considera que es necesario adoptar un enfoque unido para afrontar esa amenaza. El Reino Unido apoya la decisión de incluir una disposición en la presente Convención para sancionar la esclavitud contemporánea y la trata de personas, incluidos la trata y la explotación sexual que se cometan mediante los sitios web que ofrecen servicios para adultos.

El Reino Unido considera que el daño que causa el compartir imágenes íntimas sin autorización hace necesario que adoptemos un enfoque coordinado para prevenir ese tipo de abusos, incluso eliminando esas imágenes y asegurando que existan sanciones eficaces para quienes comparten imágenes sin autorización. El Reino Unido quisiera incluir disposiciones para afrontar ese daño.

República Unida de Tanzanía

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

4. Criminalización

Recientemente se ha producido un aumento exponencial en la utilización de las tecnologías de la información y las comunicaciones con fines delictivos por grupos de delincuentes en todo el mundo en razón del desarrollo tecnológico.

4.1 Lista de delitos

Habida cuenta de este problema, la República Unida de Tanzanía considera que es necesario que cada Estado parte apruebe las medidas legislativas y de otra índole que

resulten necesarias para tipificar como delito, cuando se cometan intencionalmente, entre otras, las siguientes acciones:

a) al acceso ilícito;

b) la interceptación ilícita;

c) la destrucción ilícita de datos electrónicos y sistemas informáticos;

d) el espionaje de datos;

e) los ataques ilícitos a la integridad del sistema;

f) la propiedad de dispositivos ilegales y/o programas informáticos con fines delictivos;

g) la falsificación y el fraude informáticos;

h) la pornografía y la pornografía infantil;

i) los delitos relacionados con la identidad;

j) la publicación de información falsa;

k) material racista o xenófobo;

l) el genocidio y los crímenes de lesa humanidad;

m) el ciberacoso;

n) la tentativa y complicidad;

o) la participación en un grupo delictivo organizado.

4.2 Responsabilidad de las personas jurídicas

La República Unida de Tanzanía propone que la convención establezca que los Estados Miembros estarán obligados a incluir, en su derecho interno, disposiciones que impongan la responsabilidad de las personas jurídicas en relación con los delitos tipificados en la convención. La responsabilidad se podrá hacer extensiva a las personas físicas que actúen en nombre de las personas jurídicas o se amparen en la personalidad de estas.

Estados Unidos de América

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

Criminalización

Tipificación de los delitos cibernéticos

“Acceso ilícito”

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito todo acceso deliberado e ilegítimo a todo o parte de un sistema informático. Los Estados partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático.

“Interceptación ilícita”

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que

transporte dichos datos informáticos. Los Estados Partes podrán exigir que el delito se cometa con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

"Ataque a la integridad de los datos"

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito, todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos.

2. Los Estados partes podrán reservarse el derecho a exigir que los actos definidos en el párrafo 1 comporten daños graves.

"Ataque a la integridad del sistema"

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.

"Uso indebido de dispositivos"

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito, la comisión deliberada e ilegítima de los siguientes actos:

a) la producción, venta, obtención para su utilización, importación, distribución o cualquier otra forma de puesta a disposición de:

i) cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos tipificados en los artículos precedentes del presente capítulo;

ii) una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático;

con intención de que sean utilizados para cometer cualquiera de los delitos tipificados en los artículos precedentes del presente capítulo, y

b) la posesión de alguno de los elementos contemplados en los incisos i) o ii) del apartado a) del presente párrafo con intención de que sean utilizados para cometer cualquiera de los delitos tipificados en los artículos precedentes del presente capítulo. Los Estados partes podrán exigir en su derecho interno la posesión de un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

2. No se interpretará que el presente artículo impone responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, distribución o cualquier otra forma de puesta a disposición o la posesión mencionada en el párrafo 1 del presente artículo no tenga por objeto la comisión de uno de los delitos previstos de conformidad con los artículos precedentes del presente capítulo, como en el caso de las pruebas autorizadas o de la protección de un sistema informático.

3. Cada Estado parte podrá reservarse el derecho a no aplicar el párrafo 1 del presente artículo, siempre que dicha reserva no afecte a la venta, distribución o cualquier otra forma de puesta a disposición de los elementos mencionados en el inciso ii) del apartado a) del párrafo 1.

"Falsificación informática"

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

partes podrán exigir que exista una intención fraudulenta o delictiva similar para que se considere que existe responsabilidad penal.

"Fraude informático"

Cada Estado parte adoptará las medidas legislativas o de otra índole que resulten necesarias para tipificar como delito la comisión deliberada e ilegítima de actos que causen perjuicio patrimonial a otra persona mediante:

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

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

con la intención fraudulenta o delictiva de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.

"Delitos informáticos relacionados con material que muestra abusos sexuales de niños"

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar las siguientes conductas, cuando se las cometa a sabiendas y mediante un sistema informático:

a) producir material que muestre la explotación sexual de niños;

b) transmitir en vivo imágenes de un niño adoptando un comportamiento sexualmente explícito;

c) ofrecer o poner a disposición material que muestre abusos sexuales de niños;

d) distribuir o transmitir material que muestre abusos sexuales de niños;

e) obtener, para uno mismo o para otras personas, material que muestre abusos sexuales de niños;

f) poseer material que muestre abusos sexuales de niños;

g) obtener acceso, a sabiendas, mediante las tecnologías de la información y las comunicaciones, de material que muestre abusos sexuales de niños o mirar la transmisión en vivo de imágenes de un niño que adopta un comportamiento sexualmente explícito.

2. Cada Estado parte adoptará las medidas legislativas o de otra índole que resulten necesarias para tipificar como delito la persuasión, la inducción, la seducción o la coacción, a sabiendas, por medio de las tecnologías de la información y las comunicaciones de un niño, o de una persona que se crea es un niño, para realizar cualquier actividad sexual ilegal. Cada Estado parte adoptará las medidas legislativas o de otra índole que resulten necesarias para que su legislación nacional no establezca que es obligatorio que el individuo y el niño se encuentren personalmente.

"Delitos informáticos relacionados con infracciones de la propiedad intelectual y de los derechos afines"

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito las infracciones de la propiedad intelectual que defina su legislación, de conformidad con las obligaciones que haya contraído en aplicación del Acta de París de 24 de julio de 1971, por la cual se revisó el Convenio de Berna para la protección de las obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la Organización Mundial de la Propiedad Intelectual (OMPI) sobre Derecho de Autor, a excepción de cualquier derecho moral otorgado por dichos tratados, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

2. Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito en su derecho interno las infracciones de los

derechos afines definidas en su legislación, de conformidad con las obligaciones que haya asumido en aplicación de la Convención Internacional sobre la Protección de los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas, a excepción de cualquier derecho moral conferido por dichos tratados, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

3. Los Estados partes podrán reservarse el derecho de no imponer responsabilidad penal en virtud de los párrafos 1 y 2 del presente artículo en circunstancias limitadas, siempre que se disponga de otros recursos efectivos y que dicha reserva no vulnere las obligaciones internacionales que incumban a dicha Parte en aplicación de los instrumentos internacionales mencionados en los párrafos 1 y 2 del presente artículo.

"Participación y tentativa"[37]

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

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

Responsabilidad de las personas jurídicas[38]

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

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

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

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

Proceso, fallo y sanciones[39]

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

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

[37] Convención de las Naciones Unidas contra la Corrupción, artículo 27.
[38] Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, artículo 10, y Convención de las Naciones Unidas contra la Corrupción, artículo 26.
[39] Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, artículo 11.

3. Cuando se trate de delitos tipificados con arreglo a los artículos sobre criminalización de la presente Convención, cada Estado parte adoptará medidas apropiadas, de conformidad con su derecho interno y tomando debidamente en consideración los derechos de la defensa, con miras a procurar que al imponer condiciones en relación con la decisión de conceder la libertad en espera de juicio o la apelación se tenga presente la necesidad de garantizar la comparecencia del acusado en todo procedimiento penal ulterior.

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

5. Cada Estado parte establecerá, cuando proceda, con arreglo a su derecho interno, un plazo de prescripción prolongado dentro del cual pueda iniciarse el proceso por cualquiera de los delitos comprendidos en la presente Convención y un plazo mayor cuando el presunto delincuente haya eludido la administración de justicia.

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

Penalización del blanqueo del producto de la ciberdelincuencia[40]

1. Cada Estado parte adoptará, de conformidad con los principios fundamentales de su derecho interno, las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito, cuando se cometan intencionalmente:

a) i) la conversión o la transferencia de bienes, a sabiendas de que esos bienes son producto del delito, con el propósito de ocultar o disimular el origen ilícito de los bienes o ayudar a cualquier persona involucrada en la comisión del delito determinante a eludir las consecuencias jurídicas de sus acciones;

ii) la ocultación o disimulación de la verdadera naturaleza, origen, ubicación, disposición, movimiento o propiedad de bienes o del legítimo derecho a estos, a sabiendas de que dichos bienes son producto del delito;

b) con sujeción a los conceptos básicos de su ordenamiento jurídico:

i) la adquisición, posesión o utilización de bienes, a sabiendas, en el momento de su recepción, de que son producto del delito;

ii) la participación en la comisión de cualesquiera de los delitos tipificados con arreglo al presente artículo, así como la asociación y la confabulación para cometerlos, el intento de cometerlos, y la ayuda, la incitación, la facilitación y el asesoramiento en aras de su comisión.

2. Para los fines de la aplicación o puesta en práctica del párrafo 1 del presente artículo:

a) Cada Estado parte incluirá como delitos determinantes los delitos tipificados con arreglo a los artículos sobre criminalización de la presente Convención. Los Estados parte cuya legislación establezca una lista de delitos determinantes incluirán entre estos, como mínimo los delitos establecidos en la presente Convención.

b) A los efectos del apartado b), los delitos determinantes incluirán los delitos cometidos tanto dentro como fuera de la jurisdicción del Estado parte interesado. No obstante, los delitos cometidos fuera de la jurisdicción de un Estado parte constituirán delito determinante siempre y cuando el acto correspondiente sea delito con arreglo al derecho interno del Estado en que se haya cometido y constituyese asimismo delito con

[40] Adaptado del artículo 6 de la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional.

arreglo al derecho interno del Estado parte que aplique o ponga en práctica el presente artículo si el delito se hubiese cometido allí.

c) Cada Estado parte proporcionará al Secretario General de las Naciones Unidas una copia de sus leyes destinadas a dar aplicación al presente artículo y de cualquier enmienda ulterior que se haga a tales leyes o una descripción de esta.

d) Si así lo requieren los principios fundamentales del derecho interno de un Estado parte, podrá disponerse que los delitos tipificados en el párrafo 1 del presente artículo no se aplicarán a las personas que hayan cometido el delito determinante.

e) El conocimiento, la intención o la finalidad que se requieren como elemento de un delito tipificado en el párrafo 1 del presente artículo podrán inferirse de circunstancias fácticas objetivas.

Penalización de la obstrucción de la justicia[41]

Cada Estado parte adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito, cuando se cometan intencionalmente:

a) El uso de fuerza física, amenazas o intimidación, o la promesa, el ofrecimiento o la concesión de un beneficio indebido para inducir a falso testimonio u obstaculizar la prestación de testimonio o la aportación de pruebas en un proceso en relación con la comisión de uno de los delitos comprendidos en la presente Convención.

b) El uso de fuerza física, amenazas o intimidación para obstaculizar el cumplimiento de las funciones oficiales de un funcionario de la justicia o de los servicios encargados de hacer cumplir la ley en relación con la comisión de los delitos comprendidos en la presente Convención. Nada de lo previsto en el presente apartado menoscabará el derecho de los Estados parte a disponer de legislación que proteja a otras categorías de funcionarios públicos.

Venezuela (República Bolivariana de)

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

5. Criminalización

La convención obligaría a los Estados parte a establecer delitos penales y de otro tipo para cubrir una amplia gama de ilícitos en lo que respecta a la utilización de las tecnologías de la información y las comunicaciones en el caso de que los que sean estipulados en la misma no constituyan ya crímenes de derecho interno. En algunos casos, los Estados tendrían la obligación legal de establecer delitos, en otros casos, con el fin de tener en cuenta las diferencias en la legislación nacional, estarían obligados a desarrollar legislación en la materia.

En tal sentido, se deben establecer claramente las actividades delictivas que se perpetran utilizando tecnologías de la información y las comunicaciones y que actualmente gozan de un amplio reconocimiento en la comunidad internacional. La convención debe ofrecer un marco orientado hacia el futuro con el fin de coordinar la tipificación de conductas, responder a las necesidades relacionadas con el desarrollo actual y ulterior de tecnologías de la información y las comunicaciones y combatir la delincuencia.

Teniendo presente lo anterior, cada Estado parte adoptará las medidas legislativas, programáticas y de otra índole que sean necesarias para tipificar los respectivos delitos. En tal sentido, habrá de preverse disposiciones que otorguen tiempo y asesoría a aquellos Estados que deban adecuar su legislación y programas nacionales.

[41] Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, artículo 23.

Los delitos principales que deben ser abarcados dentro de la convención, deben incluir los siguientes:

- Acceso indebido a la información digital que haya generado su destrucción, bloqueo o modificación.
- Intercepción premeditada de información digital sin los derechos respectivos y/o en violación de las normas establecidas, inclusive con el uso de medios técnicos de intercepción de los parámetros técnicos del tráfico y datos procesados con la utilización de las tecnologías de la información y las comunicaciones y no destinados al uso común del público.
- Manipulación ilícita de la información digital mediante su damnificación, eliminación, alteración, bloqueo, modificación de la información en formato digital.
- Hechos ilícitos premeditados para provocar un mal funcionamiento de las redes de información y las comunicaciones que entrañe consecuencias graves o que haya generado el riesgo de estas.
- Uso y distribución de programas malignos destinados para la destrucción, bloqueo, modificación y distribución no autorizados de la información digital o la neutralización de los medios de su protección.
- Creación, distribución y/o uso deliberados y premeditados de programas informáticos u otra información digital, destinados para una manipulación ilícita de la infraestructura crítica de la información, inclusive para la destrucción, bloqueo y modificación de la información contenida en esta o la neutralización de los medios de su protección.
- Creación, distribución y utilización deliberadas de programas informáticos u otra información digital concebidos con la intención de afectar indebidamente a infraestructuras de información críticas, en particular mediante la destrucción, el bloqueo, la modificación y la reproducción de la información contenida en ellos, o la neutralización de los medios de protección de la información.
- Violación de los reglamentos de explotación de los medios de almacenamiento, procesamiento y transmisión de la información digital protegida, contenida en la infraestructura crítica de la información, o de los sistemas de información, redes de información y las comunicaciones relativos a la infraestructura crítica de la información, o las normas de acceso a estas, si ha causado daños en la infraestructura crítica de la información.
- Robo de bienes o la adquisición ilícita de títulos de propiedad, incluso mediante fraude, destruyendo, bloqueando, modificando información digital o interfiriendo de otro modo en el funcionamiento de las tecnologías de la información y las comunicaciones.
- Toda exhortación, mediante la utilización de las tecnologías de la información y las comunicaciones, a cometer actos subversivos o armados que tengan por objeto el derrocamiento por la violencia del sistema de cualquier otro Estado.
- Exhortación, mediante la utilización de las tecnologías de la información y las comunicaciones, a la inducción, el reclutamiento u otra forma de involucración con fines terroristas, la propaganda y la justificación del terrorismo y la recaudación o el suministro de fondos para su financiación.
- Tráfico ilícito de estupefacientes y sustancias psicotrópicas y de los materiales necesarios para su fabricación mediante la utilización de las tecnologías de la información y las comunicaciones.
- Tráfico ilícito de armas, municiones, artefactos explosivos y explosivos mediante la utilización de las tecnologías de la información y las comunicaciones.

- Acceso no autorizado a los datos personales con el fin de destruirlos, modificarlos, copiarlos o difundirlos.
- Delitos relacionados con la producción y la circulación de materiales u objetos con representaciones pornográficas de menores cometidos mediante la utilización de las tecnologías de la información y las comunicaciones.
- Delitos relacionados con la participación de menores en la comisión de actos ilícitos peligrosos para su vida o su salud.

Viet Nam

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

Capítulo II. Criminalización

5. Cada Estado Miembro adoptará las medidas legislativas y de otra índole que resulten necesarias para tipificar como delito, cuando se cometan intencionalmente y sin autorización:

a) fabricar, comerciar, transferir instrumentos, equipos o programas informáticos destinados a atacar una red de computadoras, una red de telecomunicaciones o un dispositivo electrónico que vaya a ser utilizado para actividades delictivas según lo dispuesto en la presente Convención;

b) difundir un programa informático que es perjudicial para una red de computadoras, una red de telecomunicaciones o un dispositivo electrónico;

c) borrar, sabotear o modificar un programa informático o datos digitales;

d) obstaculizar la transmisión de datos de una red de computadoras, una red de telecomunicaciones o un dispositivo electrónico;

e) obstaculizar o alterar las operaciones normales de una red de computadoras, una red de telecomunicaciones o un dispositivo electrónico;

f) asumir control o interferir en el funcionamiento de un dispositivo electrónico eludiendo el sistema de seguridad o protección, haciendo un uso indebido de los derechos de administración de otra persona, o por cualquier otro medio;

g) robar, modificar, sabotear o falsificar información o datos;

h) utilizar una red de computadoras, una red de telecomunicaciones o un dispositivo electrónico con los fines siguientes:

i) utilizar información de una cuenta bancaria o tarjeta bancaria de una organización o una persona física para apropiarse ilegalmente de bienes;

ii) fabricar, poseer, comerciar o utilizar una tarjeta bancaria falsificada para apropiarse ilegalmente de bienes;

iii) acceder sin autorización a las cuentas de organismos de gobierno, organizaciones y personas físicas para apropiarse ilegalmente de bienes;

iv) cometer fraude en el comercio electrónico, los pagos electrónicos, el comercio de divisas, la obtención de capital en línea, el marketing multinivel o la comercialización de valores negociables en línea para apropiarse de bienes;

v) establecer o proporcionar sin autorización servicios de telecomunicaciones o de Internet para apropiarse de bienes;

i) reunir información de cuentas bancarias pertenecientes a personas físicas y organizaciones, poseerla, comerciarla, transferirla o hacerla pública;

j) comerciar, transferir, modificar o hacer pública información privada de organismos de gobierno, organizaciones o personas físicas sin el consentimiento de sus propietarios;

k) utilizar el ciberespacio, las tecnologías de la información o dispositivos electrónicos para cometer actos de terrorismo o financiar el terrorismo.

6. Nada en la presente Convención impedirá que los Estados Miembros adopten las medidas legislativas o de otra índole que resulten necesarias para tipificar como delito cualquier otro acto que implique la utilización de las tecnologías de la información y las comunicaciones con fines delictivos.

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