Naciones Unidas A/AC.291/16

Asamblea General

Distr. general
7 de noviembre de 2022
Español
Original: inglés

Comité Especial encargado de Elaborar una Convención Internacional Integral sobre la Lucha contra la Utilización de las Tecnologías de la Información y las Comunicaciones con Fines Delictivos
Cuarto período de sesiones
Viena, 9 a 20 de enero de 2023

Documento de negociación consolidado sobre las disposiciones generales y las disposiciones sobre criminalización y 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

Nota de la Presidenta

1. Como preparación para el cuarto 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 modo de trabajo del Comité Especial, aprobados en su primer período de sesiones, la Presidenta del Comité ha preparado, con el apoyo de la Secretaría, un documento de negociación consolidado elaborado sobre la base de los resultados de la primera lectura de las disposiciones generales y las disposiciones sobre criminalización y sobre medidas procesales y aplicación de la ley del proyecto de convención (véase el anexo).

2. Más concretamente, el documento de negociación consolidado se basa en diversos elementos de las propuestas de los Estados Miembros recopiladas en los documentos A/AC.291/9, A/AC.291/9/Add.1, A/AC.291/9/Add.2 y A/AC.291/9/Add.3, , así como en las declaraciones y opiniones expresadas por los Estados Miembros durante el segundo período de sesiones. Se ha intentado proponer una opción para cada disposición con elementos tomados de diferentes propuestas o declaraciones. Se han utilizado corchetes para algunos términos con el fin de reflejar las opiniones divergentes sobre su empleo expresadas por algunos Estados Miembros en los períodos de sesiones del Comité Especial.

V.22-22551 (S) 301122 301122

3. Se preparará un segundo documento de negociación consolidado sobre la base de los resultados de la primera lectura del preámbulo, las disposiciones relativas a la cooperación internacional, asistencia técnica, medidas preventivas y el mecanismo de aplicación, así como las disposiciones finales de la convención, que el Comité Especial llevó a cabo en su tercer período de sesiones; este documento se pondrá a disposición del Comité para su examen antes del quinto período de sesiones.

Anexo

Documento de negociación consolidado sobre las disposiciones generales y las disposiciones sobre criminalización y 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

Capítulo I
Disposiciones generales

Artículo 1. Finalidad

La finalidad de la presente Convención es:

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

b) promover, facilitar y reforzar la cooperación internacional para prevenir y combatir [la utilización de las tecnologías de la información y las comunicaciones con fines delictivos] [la ciberdelincuencia]; y

c) proporcionar medidas prácticas para mejorar la asistencia técnica entre los Estados partes, fomentar la capacidad de las autoridades nacionales para prevenir y combatir [la utilización de las tecnologías de la información y las comunicaciones con fines delictivos] [la ciberdelincuencia], en particular en beneficio de los países en desarrollo, y fortalecer y promover el intercambio de información, conocimientos especializados, experiencias y buenas prácticas.

Artículo 2. Definiciones

[De conformidad con las declaraciones formuladas por varios Estados Miembros en el segundo período de sesiones del Comité Especial, esta disposición debería tratarse después de que se hayan definido los principales artículos sustantivos de la Convención].

Artículo 3. Ámbito de aplicación

1. La presente Convención se aplicará, de conformidad con sus disposiciones, a la prevención, la detección, la investigación y el enjuiciamiento de [la utilización de las tecnologías de la información y las comunicaciones con fines delictivos] [la ciberdelincuencia], lo que incluye el embargo preventivo, la incautación, el decomiso y la restitución del producto de delitos tipificados con arreglo a la presente Convención.

2. La presente Convención también se aplicará a la reunión, obtención, conservación y transmisión de pruebas en formato electrónico de [los delitos tipificados con arreglo a la presente Convención] [cualquier delito] [delitos graves].

3. Para la aplicación de la presente Convención, a menos que contenga una disposición en contrario, no será necesario que los delitos enunciados en ella produzcan daño o perjuicio a personas, incluidas personas jurídicas, a bienes ni al Estado.

Artículo 4. Protección de la soberanía

1. Los Estados partes cumplirán sus obligaciones con arreglo a la presente Convención en consonancia con los principios de igualdad soberana e integridad territorial de los Estados, así como de no intervención en los asuntos internos de otros Estados.

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

Artículo 5. Respeto de los derechos humanos

1. Los Estados partes velarán por que el cumplimiento de sus obligaciones con arreglo a la presente Convención se ajuste al derecho internacional de los derechos humanos aplicable.

2. Los Estados partes se esforzarán por incorporar una perspectiva de género y por tener en cuenta las circunstancias y necesidades especiales de los grupos vulnerables, en particular las mujeres, los niños y las personas de edad, en las medidas que adopten para prevenir y combatir [la utilización de las tecnologías de la información y las comunicaciones con fines delictivos] [la ciberdelincuencia].

Capítulo II
Criminalización

GRUPO TEMÁTICO 1[1]

Artículo 6. Acceso ilícito

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito el acceso ilícito deliberado a la totalidad o una parte de un [sistema informático] [sistema/dispositivo de tecnología de la información y las comunicaciones].

2. Un Estado parte podrá exigir que el delito se cometa infringiendo las medidas de seguridad, con la intención de obtener [datos informáticos] [información electrónica/digital] u otra intención delictiva, o en relación con un [sistema informático] [sistema/dispositivo de tecnología de la información y las comunicaciones] que esté conectado a otro [sistema informático] [sistema/dispositivo de tecnología de la información y las comunicaciones].

3. Cada Estado parte podrá imponer un agravante de la pena cuando dicho acceso:

a) provoque daños a usuarios y beneficiarios;

b) dé como resultado la obtención de información gubernamental confidencial;

c) implique o afecte a infraestructuras críticas.

Artículo 7. Interceptación ilícita

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito la interceptación ilícita deliberada, por medios técnicos, de transmisiones no públicas de [datos informáticos] [información electrónica/digital] a un [sistema informático] [sistema/dispositivo de tecnología de la información y las comunicaciones], desde él o dentro de él, incluidas las emisiones electromagnéticas provenientes de un [sistema informático] [sistema/dispositivo de

[1] La organización por grupos temáticos solo tiene por objeto estructurar las deliberaciones durante las sesiones oficiales.

tecnología de la información y las comunicaciones] que transporte [esos datos informáticos] [esa información electrónica/digital].

2. Un Estado parte podrá exigir que el delito se cometa con intención dolosa, o en relación con un [sistema informático] [sistema/dispositivo de tecnología de la información y las comunicaciones] conectado a otro [sistema informático] [sistema/dispositivo de tecnología de la información y las comunicaciones].

Artículo 8. Interferencia con [datos informáticos] [información electrónica/digital]

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito todo acto deliberado e ilícito que introduzca, descargue, copie, dañe, interrumpa, borre, deteriore, altere o suprima [datos informáticos] [información electrónica/digital].

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

3. Cada Estado parte podrá imponer un agravante de la pena en caso de que los actos descritos en el párrafo 1 impliquen o afecten infraestructuras críticas.

Artículo 9. Interferencia con un [sistema informático] [sistema/dispositivo de tecnología de la información y las comunicaciones]

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito la obstaculización deliberada, grave e ilícita del funcionamiento de un [sistema informático] [sistema/dispositivo de tecnología de la información y las comunicaciones] mediante la introducción, transmisión, daño, borrado, deterioro, alteración, interrupción o supresión de [datos informáticos] [información electrónica/digital].

2. Cada Estado parte podrá imponer un agravante de la pena en caso de que los actos descritos en el párrafo 1 impliquen o afecten infraestructuras críticas.

Artículo 10. Uso indebido de dispositivos y programas

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito, cuando se cometan intencional e ilícitamente:

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, concebido o adaptado principalmente para la comisión de cualquiera de los delitos tipificados con arreglo a la presente Convención; o

ii) una contraseña, credenciales de acceso o [datos] [información] similar[es] mediante [los cuales] [la cual] se pueda acceder a la totalidad o a una parte de un [sistema informático] [sistema/dispositivo de tecnología de la información y las comunicaciones];

con la intención de que dicho dispositivo, contraseña, credenciales de acceso o [datos] [información] similar[es] se utilicen para cometer cualquiera de los delitos establecidos [en el artículo 6 sobre acceso ilícito, el artículo 7 sobre interceptación ilícita, el artículo 8 sobre interferencia con [datos informáticos] [información electrónica/digital] y el artículo 9 sobre interferencia con un [sistema informático] [sistema/dispositivo de tecnología de la información y las comunicaciones] de la presente Convención] [de conformidad con la presente Convención]; y

b) La posesión de un artículo mencionado en el párrafo 1 a) i) o ii) de este artículo, con la intención de que sea utilizado para cometer cualquiera de los delitos establecidos [en el artículo 6 sobre acceso ilícito, el artículo 7 sobre interceptación ilícita, el artículo 8 sobre interferencia con [datos informáticos] [información

electrónica/digital] y el artículo 9 sobre interferencia con un [sistema informático] [sistema/dispositivo de tecnología de la información y las comunicaciones] de la presente Convención] [de conformidad con la presente Convención]. Un Estado parte podrá 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 precedentes de] la presente Convención, como en el caso de las pruebas autorizadas o de la protección de un [sistema informático] [sistema/dispositivo de tecnología de la información y las comunicaciones].

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 párrafo 1 a) ii) del presente artículo.

GRUPO TEMÁTICO 2

Artículo 11. Falsificación [relacionada con la informática] [relacionada con las tecnologías de la información y las comunicaciones]

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito la introducción, alteración, borrado o supresión deliberados e ilegítimos de [datos informáticos] [información electrónica/digital] que genere [datos no auténticos] [información no auténtica] con la intención de que sea[n] [tomados o utilizados] [tomada o utilizada] a efectos legales como [auténticos][auténtica], con independencia de que [los datos] [la información] sea[n] legible[s] e inteligible[s] directamente, de un modo que pueda provocar daños.

2. A los fines del presente artículo, un Estado parte podrá exigir que exista la intención de defraudar o una intención delictiva similar para que se considere que existe responsabilidad penal.

Artículo 12. Fraude [relacionado con la informática] [relacionado con las tecnologías de la información y las comunicaciones]

1. Cada Estado parte adoptará las medidas legislativas o de otra índole que sean necesarias para tipificar como delito los actos de fraude deliberados e ilícitos que se hayan cometido en su totalidad o en parte en línea y causen pérdida de bienes a otra persona o a una entidad mediante:

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

b) la interferencia con el funcionamiento de un [sistema informático] [sistema/dispositivo de tecnología de la información y las comunicaciones];

c) el uso de un [sistema informático] [sistema/dispositivo de tecnología de la información y las comunicaciones] para engañar o inducir a otra persona o a una entidad para que haga o deje de hacer algo que la persona o entidad no haría o dejaría de hacer de otro modo,

con la intención fraudulenta o delictiva de obtener de forma ilegítima para uno mismo o para otra persona:

i) un beneficio económico; o

ii) [datos informáticos] [información electrónica/digital], [incluidos datos personales] [incluida información personal] que el autor del acto no tendría a su disposición de otro modo.

2. Los actos de fraude incluyen, entre otras, las actividades que se realicen en el país o a través de las fronteras por Internet u otros medios [basados en la cibernética] [digitales], con los siguientes métodos:

a) fraude cometido mediante una representación engañosa;

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

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

Artículo 13. Robo [relacionado con la informática] [relacionado con las tecnologías de la información y las comunicaciones]

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito el robo de bienes o la adquisición ilícita de derechos sobre ellos, mediante la destrucción, el bloqueo, la modificación o la copia de [datos informáticos] [información electrónica/digital] u otro modo de interferencia en el funcionamiento de las operaciones [informáticas] [de tecnologías de la información y las comunicaciones].

2. Cada Estado parte podrá considerar el robo de bienes o la adquisición ilícita de derechos sobre ellos relacionados con [la informática] [la tecnología de la información y las comunicaciones] como una circunstancia agravante del delito de robo definido en su derecho interno.

Artículo 14. Utilización ilícita de instrumentos de pago electrónicos

Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito los siguientes actos:

a) la falsificación, fabricación o instalación de cualquier dispositivo o material que facilite la falsificación o imitación de instrumentos electrónicos de pago por cualquier medio;

b) la apropiación, utilización o suministro a otras personas de [los datos] [la información] de cualquier instrumento de pago o la facilitación de la obtención por otras personas de [dichos datos] [dicha información];

c) la utilización de [una red de información o la tecnología de la información] [un sistema informático] para tener acceso no autorizado a [datos] [información] de cualquier instrumento de pago;

d) la aceptación a sabiendas de un instrumento de pago falsificado.

GRUPO TEMÁTICO 3

Artículo 15. Violación de la información personal

Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito, cuando se cometan de manera intencional e ilícita, el acceso, la venta, el suministro o la puesta a disposición de otro modo de cualquier material que contenga información personal sobre una persona, incluida información relacionada con su cuenta bancaria, con la intención de obtener un beneficio económico, y la posterior divulgación de dicho material a cualquier otra persona sin el consentimiento de la persona afectada.

Artículo 16. Delitos relacionados con la identidad

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

a) la obtención, recepción o distribución ilegítimas de contraseñas o credenciales de acceso a [un sistema informático] [datos informáticos]; y

b) el uso fraudulento o deshonesto de la firma electrónica, la contraseña o cualquier otro elemento único de identificación de cualquier otra persona.

GRUPO TEMÁTICO 4

Artículo 17. Violación del derecho de autor

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito, cuando se cometa intencionalmente, la violación del derecho de autor, tal como se define en la legislación de ese Estado parte, por medio de un [sistema informático] [sistema/dispositivo de tecnología de la información y las comunicaciones], incluida la utilización ilícita de programas informáticos y bases de datos protegidos por el derecho de autor, y el plagio, de conformidad con las obligaciones que haya contraído en virtud de los tratados pertinentes y aplicables, con excepción de cualquier derecho moral conferido por dichos tratados, cuando esos actos se cometan deliberadamente y a escala comercial.

2. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito, cuando se cometan intencionalmente, las violaciones de derechos relacionados con el derecho de autor que defina su legislación cometidas por medio de un [sistema informático] [sistema/dispositivo de tecnología de la información y las comunicaciones], de conformidad con las obligaciones que haya contraído en aplicación de los tratados pertinentes y aplicables, 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] [sistema/dispositivo 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 en circunstancias limitadas, siempre que se disponga de otros recursos efectivos y que dicha reserva no vulnere las obligaciones internacionales que incumban al Estado parte.

GRUPO TEMÁTICO 5

Artículo 18. Delitos relacionados con material en línea que muestra abusos o explotación sexuales de niños

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito, cuando se cometan de manera intencional e ilícita, las conductas siguientes:

a) producir o reproducir material que muestre abusos o explotación sexuales de niños a fines de su distribución mediante un [sistema informático] [sistema/dispositivo de tecnología de la información y las comunicaciones];

b) financiar o facilitar de otro modo material que muestre abusos o explotación sexuales de niños mediante un [sistema informático] [sistema/dispositivo de tecnología de la información y las comunicaciones];

c) controlar, promover, ofrecer, publicitar, mostrar públicamente o poner a disposición material que muestre abusos o explotación sexuales de niños mediante un [sistema informático] [sistema/dispositivo de tecnología de la información y las comunicaciones];

d) distribuir o transmitir material que muestre abusos o explotación sexuales de niños mediante un [sistema informático] [sistema/dispositivo de tecnología de la información y las comunicaciones];

e) adquirir material que muestre abusos o explotación sexuales de niños mediante un [sistema informático] [sistema/dispositivo de tecnología de la información y las comunicaciones];

f) obtener a sabiendas el acceso o la posesión de material que muestre abusos o explotación sexuales de niños en un [sistema informático] [sistema/dispositivo de tecnología de la información y las comunicaciones] o un [medio de almacenamiento de datos informáticos] [dispositivo de almacenamiento de datos digitales/electrónicos] o ver la transmisión en vivo de la participación de niños en conductas sexualmente explícitas;

g) participar en los beneficios derivados de toda actividad comercial que, por lo que la persona sabe o tiene motivos para creer, guarda relación con cualquier material que muestre abusos o explotación sexuales de niños mediante un [sistema informático] [sistema/dispositivo de tecnología de la información y las comunicaciones] o percibir dichos beneficios.

2. A efectos del apartado 1, el término “material que muestre abusos o explotación sexuales de niños” incluirá el material visual, incluidos medios fotográficos, de video y de transmisión en directo, así como dibujos, material escrito y grabaciones de audio, que representen:

a) a un niño que exhiba un comportamiento sexualmente explícito real o simulado;

b) a una persona que parezca un niño que exhiba un comportamiento sexualmente explícito real o simulado;

c) imágenes realistas de un niño que exhiba un comportamiento sexualmente explícito real o simulado;

d) cualquier representación de los órganos sexuales de un niño con fines principalmente sexuales;

e) a una víctima de tortura u otros tratos o penas crueles, inhumanos o degradantes.

3. A los efectos del párrafo 2, se entenderá por “niño” toda persona menor de 18 años de edad.

4. Los Estados partes tendrán debidamente en cuenta la necesidad de evitar la criminalización de los niños que hayan generado por sí mismos material descrito en el párrafo 2, así como la necesidad de respetar las obligaciones que les incumben en virtud de la Convención sobre los Derechos del Niño y sus Protocolos.

5. Cada Estado parte podrá reservarse el derecho a no aplicar, en todo o en parte, lo dispuesto en el párrafo 1 e) y f) y el párrafo 2 b) y c).

Artículo 19. Facilitación mediante un [sistema informático] [sistema/dispositivo de tecnología de la información y las comunicaciones] de material que muestre abusos o explotación sexuales de niños

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito en su derecho interno todo acto deliberado y sin motivo lícito que cree, desarrolle, altere, mantenga, controle, modere, asista, ponga a disposición, publicite o promueva un [sistema informático] [sistema/dispositivo de tecnología de la información y las comunicaciones] con el fin de facilitar material que muestre abusos o explotación sexuales de niños en los términos definidos en el artículo 18 de la presente Convención.

2. A los efectos del párrafo 1, por la expresión “facilitación de material que muestre abusos o explotación sexuales 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 o explotación sexuales de niños, producirlo o transmitir, distribuir, ofrecer o poner a disposición ese tipo de material para sí mismas u otras personas.

Artículo 20. Captación u obtención de niños con fines sexuales mediante un [sistema informático] [sistema/dispositivo de tecnología de la información y las comunicaciones]

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito, cuando se cometan intencionalmente, la captación, el acuerdo, la concertación, la proposición, la obtención, la instigación, la coerción o [la inducción] [la atracción] de un niño, con el fin de facilitar, alentar, ofrecer o instigar conductas sexuales ilícitas de un niño o una persona que se crea que es un niño o con él, o hacer que este presencie actividades sexuales a través de [un sistema informático] [un sistema/dispositivo de tecnología de la información y las comunicaciones] o participe de otro modo en estas actividades.

2. A efectos del apartado 1, se aplicará el artículo 2 [(x)] [relativo a la definición de “niño” y la responsabilidad penal de los niños]. Además, la palabra “niño” también incluye a una persona que se crea es menor de 18 años.

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

Artículo 21. Ciberhostigamiento de un niño

Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito la utilización deliberada de un [sistema informático] [sistema/dispositivo de tecnología de la información y las comunicaciones] para recopilar, transmitir, publicar, reproducir, comprar, vender, recibir, intercambiar o difundir el nombre, número de teléfono, dirección de correo electrónico, domicilio, fotografía, descripción física, características o cualquier otra información que identifique a un niño con el objetivo de tratar de concertar un encuentro con él con el fin de mantener relaciones sexuales, adoptar una conducta sexualmente explícita o realizar actividades sexuales ilícitas.

GRUPO TEMÁTICO 6

Artículo 22. Implicación de menores en la comisión de actos ilícitos

Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito el uso de un [sistema informático] [sistema/dispositivo de tecnología de la información y las comunicaciones] para implicar a menores en la comisión de actos ilícitos que pongan en peligro su vida o su salud física o mental, con excepción de los actos previstos en el artículo [23] [, relativo a la incitación o coerción para cometer suicidio,] de la presente Convención.

Artículo 23. Incitación o coerción para cometer suicidio

Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito la incitación o la coerción para cometer suicidio, incluso de niños, mediante presión psicológica o de otro tipo aplicada a través del uso de un [sistema informático] [sistema/dispositivo de tecnología de la información y las comunicaciones].

GRUPO TEMÁTICO 7

Artículo 24. Extorsión sexual

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito las amenazas deliberadas de distribuir o transmitir, por medios electrónicos, una imagen de carácter íntimo de otra persona, con la intención específica de:

a) acosar, amenazar, ejercer coerción, intimidar o ejercer influencia indebida sobre la persona, especialmente para obtener un beneficio económico u otro beneficio de orden material, lo que incluye el fin de obligar a la víctima a realizar actividades sexuales no deseadas; o

b) obtener un beneficio económico u otro beneficio de orden material, lo que incluye el fin de obligar a la víctima a realizar actividades sexuales no deseadas.

2. A los efectos del párrafo 1, por "imagen de carácter íntimo" se entenderá un registro visual de una persona captado por cualquier medio, con inclusión de un registro fotográfico, fílmico o videográfico:

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

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

c) respecto del cual la persona representada seguía teniendo una expectativa razonable de privacidad en el momento en que se cometió el delito.

Artículo 25. Diseminación no consentida de imágenes de carácter íntimo

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito, cuando se cometan de manera intencional e ilícita, la publicación, distribución, transmisión, venta, puesta a disposición o publicidad de una imagen de carácter íntimo de una persona por medio de un [sistema informático] [sistema/dispositivo de tecnología de la información y las comunicaciones], [con la intención de causar un malestar emocional grave] 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 de carácter íntimo" se entenderá un registro visual de una persona captado por cualquier medio, con inclusión de un registro fotográfico, fílmico o videográfico:

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

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

c) respecto del cual la persona representada seguía teniendo una expectativa razonable de privacidad en el momento en que se cometió el delito.

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

4. Un niño no puede consentir a la publicación de una imagen de carácter íntimo de la que es sujeto.

GRUPO TEMÁTICO 8

Artículo 26. Incitación a cometer actos subversivos o armados

Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito en su legislación nacional 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 régimen de otro Estado.

Artículo 27. Delitos relacionados con el extremismo

Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito la distribución de material que exhorte a la comisión de actos ilícitos motivados por el odio político, ideológico, social, racial, étnico o religioso, la promoción y la justificación de esos actos y la facilitación de acceso a ese material mediante un [sistema informático] [sistema/dispositivo de tecnología de la información y las comunicaciones].

Artículo 28. Denegación, aprobación, justificación o rehabilitación 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 sean necesarias para tipificar como delito en su legislación nacional la difusión deliberada relacionada con [medios informáticos] [las tecnologías de la información y las comunicaciones] de material que niegue, apruebe, justifique o rehabilite 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.

GRUPO TEMÁTICO 9

Artículo 29. Delitos relacionados con el terrorismo

Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito, cuando se lleven a cabo por medio de las tecnologías de la información y las comunicaciones, la comisión de actos terroristas, la incitación, el reclutamiento o la participación de otro tipo en actividades terroristas, la apología y la justificación del terrorismo o la recaudación o el suministro de fondos para su financiación, el adiestramiento para la comisión de actos terroristas, la facilitación de la comunicación entre las organizaciones terroristas y sus miembros, incluidos el establecimiento, la publicación o la utilización de un sitio web o el suministro de apoyo logístico a los autores de actos terroristas, la difusión de métodos para la fabricación de explosivos empleados en particular en actos terroristas y la difusión de la lucha, la sedición, el odio o el racismo.

Artículo 30. Delitos relacionados con la distribución de estupefacientes y sustancias sicotrópicas

Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito, cuando se cometa intencionalmente, el tráfico ilícito de estupefacientes y sustancias sicotrópicas y del material necesario para su fabricación mediante la utilización de un [sistema/dispositivo de tecnología de la información y las comunicaciones] [sistema informático].

Artículo 31. Delitos relacionados con el tráfico de armas

Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito, cuando se cometa intencionalmente, el tráfico ilícito de armas de fuego, municiones, artefactos explosivos y sustancias explosivas en que se utilicen tecnologías de la información y las comunicaciones.

Artículo 32. Distribución ilícita de medicamentos y productos médicos falsificados

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

GRUPO TEMÁTICO 10

Artículo 33. 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 sean necesarias para tipificar como delito, cuando se cometan intencionalmente:

a) i) la conversión o la transferencia de bienes, incluidas monedas virtuales, 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 actos;

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 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 los delitos pertinentes tipificados con arreglo a la presente Convención. Los Estados partes cuya legislación establezca una lista de delitos determinantes incluirán entre estos, como mínimo, una amplia gama de delitos relacionados con [la utilización de las tecnologías de la información y las comunicaciones con fines delictivos] [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.

Artículo 34. Obstrucción de la justicia

Cada Estado parte adoptará las medidas legislativas y de otra índole que sean 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 partes a disponer de legislación que proteja a otras categorías de funcionarios públicos.

GRUPO TEMÁTICO 11

Artículo 35. Responsabilidad de las personas jurídicas

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias, de conformidad con sus normas jurídicas, a fin de establecer la responsabilidad de personas jurídicas 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 Estado parte adoptará las medidas necesarias para garantizar que pueda exigirse responsabilidad a una persona jurídica cuando la ausencia de vigilancia o de control por parte de cualquier persona física mencionada en el párrafo 1 haya permitido la comisión de un delito tipificado con arreglo a la presente Convención por una persona física que actúe en beneficio de dicha persona jurídica y bajo su autoridad expresa o tácita.

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

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

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

6. 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.

Artículo 36. Participación y tentativa

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para tipificar como delito, de conformidad con su derecho interno, cualquier forma de participación, ya sea como cómplice, colaborador, instigador, promotor o confabulador, en un delito tipificado con arreglo a la presente Convención, o la organización o la impartición de instrucciones a otras personas para que cometan un delito tal.

2. Cada Estado parte podrá adoptar las medidas legislativas y de otra índole que sean necesarias para tipificar como delito, de conformidad con su derecho interno, cuando se cometa intencionalmente, toda tentativa de cometer un delito tipificado con arreglo a la presente Convención.

3. Cada Estado parte podrá adoptar las medidas legislativas y de otra índole que sean necesarias para tipificar como delito, de conformidad con su derecho interno, cuando se cometa intencionalmente, todo preparativo para cometer un delito tipificado con arreglo a la presente Convención.

4. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para reforzar la responsabilidad por los delitos colectivos, incluidos los perpetrados por grupos delictivos organizados.

5. Cada Estado parte podrá reservarse el derecho a no aplicar, en todo o en parte, lo dispuesto en el párrafo 2 del presente artículo.

Artículo 37. Conocimiento, intención y propósito como elementos de un delito

El conocimiento, la intención o el propósito que se requieren como elemento de un delito tipificado con arreglo a la presente Convención podrán inferirse de circunstancias fácticas objetivas.

Artículo 38. Prescripción

Cada Estado parte establecerá, cuando proceda, con arreglo a su derecho interno, un plazo de prescripción amplio para iniciar procesos por cualesquiera de los delitos tipificados con arreglo a la presente Convención y establecerá un plazo mayor o interrumpirá la prescripción cuando el presunto delincuente haya eludido la administración de justicia.

Artículo 39. Proceso, fallo y sanciones

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

2. Cada Estado parte podrá imponer una agravación de la pena por los delitos tipificados con arreglo a la presente Convención, incluidos, entre otros, los casos en que la comisión de los delitos:

a) afecte a infraestructuras críticas;

b) dé como resultado la obtención de información gubernamental confidencial;

c) cause daños, físicos o psicológicos, a las personas.

3. Cada Estado parte adoptará las medidas que sean necesarias para establecer o mantener, de conformidad con su ordenamiento jurídico y sus principios constitucionales, un equilibrio apropiado entre cualesquiera inmunidades o prerrogativas jurisdiccionales otorgadas a sus funcionarios públicos para el cumplimiento de sus funciones y la posibilidad, de ser preciso, de proceder efectivamente a la investigación, el enjuiciamiento y el fallo de los delitos tipificados con arreglo a la presente Convención.

4. 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 tipificados con arreglo a 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.

5. Cada Estado parte velará por que toda persona procesada por delitos tipificados con arreglo a la presente Convención goce de todos los derechos y garantías de conformidad con la legislación del Estado en cuyo territorio se encuentre y con las disposiciones pertinentes y aplicables del derecho internacional de los derechos humanos, incluido el derecho a un juicio imparcial y el derecho de defensa.

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

7. Cada Estado parte tendrá en cuenta la gravedad de los delitos pertinentes al considerar la eventualidad de conceder la libertad anticipada o la libertad condicional a personas que hayan sido declaradas culpables de esos delitos.

8. 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 partes y de que esos delitos habrán de ser perseguidos y sancionados de conformidad con ese derecho.

9. Los Estados partes procurarán promover la reinserción social de las personas condenadas por delitos tipificados con arreglo a la presente Convención.

Capítulo III
Medidas procesales y aplicación de la ley

GRUPO TEMÁTICO 1

Artículo 40. Jurisdicción

1. Cada Estado parte adoptará las medidas que sean 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 el artículo 4 de la presente Convención, un Estado parte también podrá establecer su jurisdicción para conocer de tales delitos cuando:

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

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

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

d) el delito se cometa contra el Estado parte; o

e) el delito implique [datos informáticos] [información electrónica/digital] de nacionales del Estado parte, con independencia del lugar en que se almacene[n] físicamente, procese[n] o examine[n].

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

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

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.

Artículo 41. Ámbito de aplicación de las medidas procesales

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

2. Salvo que se establezca lo contrario en el artículo 48 de la presente Convención, cada parte aplicará las facultades y procedimientos mencionados en el párrafo 1 del presente artículo:

a) a los delitos tipificados con arreglo a la presente Convención;

b) a cualquier otro delito cometido mediante un [sistema informático] [sistema/dispositivo de tecnologías de la información y las comunicaciones]; y

c) la obtención de pruebas en forma electrónica de [delitos tipificados con arreglo a la presente Convención] [cualquier delito] [delitos graves].

3. a) Cada Estado parte podrá reservarse el derecho a aplicar las medidas mencionadas en el artículo 47 de la presente Convención únicamente a los delitos o categorías de delitos especificados en su reserva, siempre que la gama de dichos delitos o categorías de delitos no sea más reducida que la de los delitos a los que dicho Estado parte aplique las medidas mencionadas en el artículo 48. Cada Estado parte tratará de limitar tal reserva de modo que sea posible la más amplia aplicación de las medidas de obtención en tiempo real de datos relativos al tráfico.

b) Cuando, a causa de las restricciones que imponga su legislación vigente en el momento de la adopción de la presente Convención, un Estado parte no pueda aplicar las medidas en materia de obtención en tiempo real de datos relativos al tráfico y de interceptación de datos relativos al contenido a las comunicaciones transmitidas dentro de un [sistema informático] [sistema/dispositivo de tecnología de la información y las comunicaciones] de un proveedor de servicios:

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

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

dicho Estado parte podrá reservarse el derecho a no aplicar estas medidas a esas comunicaciones. Cada Estado parte tratará de limitar tal reserva de modo que sea posible la más amplia aplicación de las medidas de obtención en tiempo real de datos relativos al tráfico y de interceptación de datos relativos al contenido.

Artículo 42. Condiciones y salvaguardias

1. Cada Estado parte se asegurará de que la instauración, ejecución y aplicación de las facultades y procedimientos previstos en el presente capítulo se sometan a las condiciones y salvaguardias previstas en su derecho interno, que deberá garantizar una protección adecuada de los derechos humanos y de las libertades, y en particular de los derechos y libertades fundamentales derivados de las obligaciones que haya asumido en virtud del derecho internacional de los derechos humanos aplicable y que deberá integrar los principios de proporcionalidad, necesidad y legal y la protección de la privacidad y de los datos personales.

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

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

GRUPO TEMÁTICO 2

Artículo 43. Conservación rápida de [datos informáticos almacenados] [información electrónica/digital acumulada]

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para que sus autoridades competentes puedan dictar órdenes o instrucciones adecuadas u obtener o garantizar de forma análoga la conservación rápida de [datos informáticos específicos] [información electrónica/digital específica], con inclusión de datos relativos al tráfico, que se haya[n] almacenado mediante un [sistema informático] [sistema/dispositivo de tecnología de la información y las comunicaciones], sobre todo cuando haya motivos para creer que [los datos informáticos son particularmente susceptibles de ser borrados, copiados, perdidos o modificados] [la información electrónica/digital es particularmente susceptible de ser borrada, copiada, perdida o modificada], en particular a raíz de la expiración del período de conservación previsto en su legislación nacional o las condiciones de servicio del proveedor.

2. Cuando un Estado parte aplique lo dispuesto en el párrafo 1 por medio de una orden impartida a una persona, incluidas personas jurídicas, a efectos de que conserve [determinados datos informáticos almacenados] [determinada información electrónica/digital almacenada] que se encuentre[n] en poder o bajo el control de esa persona, el Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para obligar a dicha persona a conservar y a proteger la integridad de [esos datos informáticos] [esa información electrónica/digital] durante el tiempo necesario, hasta un máximo de 90 días, con el fin de que las autoridades competentes puedan obtener su revelación. Todo Estado parte podrá prever la renovación de dicha orden.

3. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para obligar al custodio u otra persona que deba conservar [los datos informáticos] [la información electrónica/digital] a mantener la confidencialidad de la realización de dichos procedimientos durante el período de tiempo previsto por su legislación nacional.

4. Las facultades y procedimientos mencionados en el presente artículo se establecerán de conformidad con lo dispuesto en los artículos 41 y 42 de la presente Convención.

Artículo 44. Conservación y revelación parcial rápidas de los datos relativos al tráfico.

1. Cada Estado parte adoptará, en relación con los datos relativos al tráfico que hayan de preservarse en virtud de las disposiciones del artículo referido a la conservación rápida de [los datos informáticos] [la información electrónica/digital], las medidas legislativas y de otra índole que sean necesarias para:

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

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

2. Las facultades y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 41 y 42.

Artículo 45. Orden de presentación

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

a) a una persona presente en su territorio que comunique [determinados datos informáticos] [determinada información electrónica/digital] que se halle[n] en su poder o bajo su control y que esté[n] [almacenados] [almacenada] en un sistema informático o en un dispositivo de almacenamiento de datos informáticos; y

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

2. Las facultades y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 41 y 42.

3. A los efectos del presente artículo, se entenderá por “datos relativos a los abonados” cualquier información, en forma de [datos informáticos] [información electrónica/digital] o de cualquier otro modo, que posea un proveedor de servicios y que se refiera a los abonados de sus servicios, aparte de los datos relativos al tráfico o al contenido, y que permita[n] determinar:

a) el tipo de servicio de tecnología de la información y las comunicaciones utilizado, las disposiciones técnicas aplicadas al respecto y el período de servicio;

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

c) información relativa a la ubicación del equipo de información y comunicaciones disponible de conformidad con el contrato o acuerdo de prestación de servicio.

Artículo 46. Registro y embargo de [información almacenada o procesada electrónicamente/digitalmente][datos informáticos almacenados]

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para facultar a sus autoridades competentes, cuando existan motivos razonables para creer que se ha cometido o se está cometiendo un delito, a registrar o acceder de manera similar en el territorio o bajo la jurisdicción de ese Estado parte:

a) a un [sistema/dispositivo de tecnología de la información y las comunicaciones] [sistema informático], parte de él y a [los datos informáticos allí almacenados] [la información electrónica/digital allí almacenada]; y

b) a un medio de almacenamiento de [datos informáticos] [información electrónica/digital] en el que pueda[n] estar [almacenados los datos informáticos] [almacenada la información electrónica/digital] que se busque[n].

2. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para asegurarse de que, cuando sus autoridades competentes que realicen un registro de conformidad con lo dispuesto en el párrafo 1 a) del presente artículo tengan motivos razonables para creer que [los datos informáticos] [la información electrónica/digital] que buscan está[n] [almacenados] [almacenada] en otro [sistema/dispositivo de tecnología de la información y las comunicaciones] [sistema informático] situado en territorio del Estado parte y pueda accederse legalmente a [esos datos] [esa información] o disponerse de [ellos] [ella] desde el sistema inicial, dichas autoridades puedan proceder rápidamente al registro para acceder a ese otro [sistema/dispositivo de tecnología de la información y las comunicaciones] [sistema informático] o a [los datos allí almacenados] [la información allí almacenada].

3. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para facultar a sus autoridades competentes a embargar u obtener de manera similar [los datos informáticos] [la información electrónica/digital] presente[s] en su territorio o [sujetos] [sujeta] a su jurisdicción a que se haya tenido acceso de conformidad con los párrafos 1 o 2 u [obtenerlos] [obtenerla] de un modo similar. Estas medidas incluirán la facultad de:

a) embargar u obtener de otra manera un [sistema/dispositivo de tecnología de la información y las comunicaciones] [sistema informático], parte de él o un medio utilizado para almacenar [datos informáticos] [información electrónica/digital];

b) hacer y conservar copias de [esos datos informáticos] [esa información electrónica/digital] en formato electrónico/digital;

c) mantener la integridad de [los datos informáticos almacenados pertinentes] [la información electrónica/digital almacenada pertinente];

d) imposibilitar el acceso a [los datos informáticos] [la información electrónica/digital] del [sistema informático] [sistema/dispositivo de tecnología de la información y las comunicaciones] consultado o [suprimirlos] [suprimirla].

4. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para facultar a sus autoridades competentes a ordenar a toda persona provista de conocimientos especiales sobre el funcionamiento del [sistema/dispositivo de tecnología de la información y las comunicaciones] [sistema informático] en cuestión, la red de información y telecomunicaciones o sus componentes o las medidas aplicadas para proteger [los datos informáticos] [la información electrónica/digital] que figura[n] en ellos que proporcione, en la medida de lo razonable, la información necesaria para que puedan aplicarse las medidas indicadas en los párrafos 1 a 3 del presente artículo.

5. Las facultades y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 41 y 42.

Artículo 47. Obtención en tiempo real de datos relativos al tráfico

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para facultar a sus autoridades competentes, cuando exista la creencia razonable de que se ha cometido o se está cometiendo un delito, para llevar a cabo las siguientes acciones con respecto a los datos relativos al tráfico asociados a determinadas comunicaciones en su territorio transmitidas por medio de un [sistema informático] [sistema/dispositivo de tecnología de la información y las comunicaciones] en el territorio de ese Estado parte:

a) obtener o grabar, en tiempo real, con los medios técnicos existentes en su territorio; y

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

i) obtener o grabar, en tiempo real, con los medios técnicos existentes en su territorio; o

ii) prestar a las autoridades competentes su colaboración y su asistencia para obtener o grabar, en tiempo real,

esos datos asociados a información específica transmitida en su territorio.

2. Cuando un Estado parte, debido a los principios fundamentales de su ordenamiento jurídico interno, no pueda adoptar las medidas a que se refiere el párrafo 1 a), podrá adoptar en su lugar las medidas legislativas y de otra índole que sean necesarias para garantizar la recopilación o el registro en tiempo real del tráfico de datos asociados con comunicaciones específicas transmitidas en su territorio, mediante la aplicación de medios técnicos en ese territorio.

3. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para obligar a un proveedor de servicios a mantener confidencial el hecho de la ejecución de cualquier facultad prevista en este artículo y cualquier información relacionada con ella.

4. Las facultades y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 41 y 42.

Artículo 48. Interceptación de datos relativos al contenido

1. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias, en lo que respecta a una gama de delitos graves que deberá definirse en su derecho interno, para facultar a sus autoridades competentes a llevar a cabo las siguientes acciones con respecto a [datos relativos al contenido] [información electrónica/digital, incluidos datos relativos al contenido, transmitida mediante tecnologías de la información y las comunicaciones] de determinadas comunicaciones transmitidas mediante un [sistema informático] [sistema/dispositivo de tecnología de la información y las comunicaciones] en su territorio:

a) obtener o grabar, en tiempo real, con los medios técnicos existentes en su territorio; y

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

i) obtener o grabar, en tiempo real, con los medios técnicos existentes en su territorio; o

ii) prestar a las autoridades competentes cooperación y asistencia para la reunión o el registro, en tiempo real,

de [dichos datos] [dicha información].

2. Cuando un Estado parte, debido a los principios fundamentales de su ordenamiento jurídico interno, no pueda adoptar las medidas a que se refiere el párrafo 1 a), podrá adoptar en su lugar las medidas legislativas y de otra índole que sean necesarias para garantizar la recopilación o el registro en tiempo real del tráfico de datos relativos al contenido de comunicaciones específicas en su territorio, mediante la aplicación de medios técnicos en ese territorio.

3. Cada Estado parte adoptará las medidas legislativas y de otra índole que sean necesarias para obligar a un proveedor de servicios a mantener confidencial el hecho de la ejecución de cualquier facultad prevista en este artículo y cualquier información relacionada con ella.

4. Las facultades y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 41 y 42.

Artículo 49. Admisión de pruebas [digitales][electrónicas]

Las pruebas [digitales][electrónicas] derivadas o extraídas de dispositivos, equipos, medios [digitales][electrónicas], sistemas de información, programas informáticos o cualquier tecnología de la información y las comunicaciones tendrán el mismo valor probatorio que las pruebas forenses materiales en los procedimientos penales cuando dichas pruebas cumplan las condiciones técnicas previstas por las leyes de los Estados partes en cuestión.

GRUPO TEMÁTICO 3

Artículo 50. Embargo preventivo, incautación y decomiso del producto del delito

1. Cada Estado parte adoptará, en la medida en que lo permita su ordenamiento jurídico interno, las medidas que sean necesarias para autorizar el decomiso:

a) del producto de delitos tipificados con arreglo a la presente Convención o de bienes cuyo valor corresponda al de dicho producto;

b) de los bienes, equipo u otros instrumentos utilizados o destinados a utilizarse en la comisión de los delitos tipificados con arreglo a la presente Convención.

2. Cada Estado parte adoptará las medidas que sean necesarias para permitir la identificación, la localización, el embargo preventivo o la incautación de cualquier bien a que se haga referencia en el párrafo 1 del presente artículo con miras a su eventual decomiso.

3. Cada Estado parte adoptará, de conformidad con su derecho interno, las medidas legislativas y de otra índole que sean necesarias para regular la administración, por parte de las autoridades competentes, de los bienes embargados, incautados o decomisados comprendidos en los párrafos 1 y 2 del presente artículo.

4. Cuando el producto del delito se haya transformado o convertido parcial o totalmente en otros bienes, esos bienes podrán ser objeto de las medidas aplicables a dicho producto a tenor del presente artículo.

5. Cuando el producto del delito se haya mezclado con bienes adquiridos de fuentes lícitas, esos bienes podrán, sin menoscabo de cualquier otra facultad de embargo preventivo o incautación, ser objeto de decomiso hasta el valor estimado del producto entremezclado.

6. Los ingresos u otros beneficios derivados del producto del delito, de bienes en los que se haya transformado o convertido el producto del delito o de bienes con los que se haya entremezclado el producto del delito también podrán ser objeto de las medidas previstas en el presente artículo, de la misma manera y en el mismo grado que el producto del delito.

7. Para los fines del presente artículo y del artículo de la presente Convención [relativo a la cooperación internacional con fines de decomiso], cada Estado parte facultará a sus tribunales u otras autoridades competentes para ordenar la presentación o la incautación de documentos bancarios, financieros o comerciales. Los Estados partes no podrán negarse a aplicar las disposiciones del presente párrafo amparándose en el secreto bancario.

8. Cada Estado parte podrá considerar la posibilidad de exigir a un delincuente que demuestre el origen lícito del presunto producto del delito o de otros bienes expuestos a decomiso, en la medida en que ello sea conforme con los principios de su derecho interno y con la índole del proceso judicial u otras actuaciones conexas.

9. Las disposiciones del presente artículo no se interpretarán en perjuicio de los derechos de terceros de buena fe.

10. Nada de lo dispuesto en el presente artículo afectará al principio de que las medidas en él previstas se definirán y aplicarán de conformidad con el derecho interno de los Estados partes.

Artículo 51. Establecimiento de antecedentes penales

Cada Estado parte podrá adoptar las medidas legislativas o de otra índole que sean necesarias para tener en cuenta, en las condiciones y para los fines que estime apropiados, toda previa declaración de culpabilidad de un presunto delincuente en otro Estado a fin de utilizar esa información en actuaciones penales relativas a delitos tipificados con arreglo a la presente Convención.

Artículo 52. Protección de los testigos

1. Cada Estado parte adoptará medidas apropiadas dentro de sus posibilidades para proteger de manera eficaz contra eventuales actos de represalia o intimidación a los testigos que presten testimonio o proporcionen información, de buena fe y con motivos razonables, sobre delitos comprendidos en la presente Convención o cooperen de otro modo con las autoridades investigadoras o judiciales, así como, cuando proceda, a sus familiares y demás personas cercanas.

2. Las medidas previstas en el párrafo 1 del presente artículo podrán consistir, entre otras, sin perjuicio de los derechos del acusado, incluido el derecho a las garantías procesales, en:

a) establecer procedimientos para la protección física de esas personas, incluida, en la medida de lo necesario y lo posible, su reubicación, y permitir, cuando proceda, la prohibición total o parcial de revelar información relativa a su identidad y paradero;

b) establecer normas probatorias que permitan que el testimonio de los testigos se preste de modo que no se ponga en peligro su seguridad, por ejemplo aceptando el testimonio por conducto de tecnologías de comunicación como videoconferencias u otros medios adecuados.

3. Los Estados partes considerarán la posibilidad de celebrar acuerdos o arreglos con otros Estados para la reubicación de las personas mencionadas en el párrafo 1 del presente artículo.

4. Las disposiciones del presente artículo también serán aplicables a las víctimas en el caso de que actúen como testigos.

Artículo 53. Asistencia y protección a las víctimas

1. Cada Estado parte adoptará medidas apropiadas dentro de sus posibilidades para prestar asistencia y protección a las víctimas de los delitos tipificados con arreglo a la presente Convención, en particular en casos de amenaza de represalia o intimidación.

2. Cada Estado parte establecerá procedimientos adecuados que permitan a las víctimas de los delitos tipificados con arreglo a la presente Convención obtener indemnización y restitución.

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

Artículo 54. Indemnización por daños y perjuicios

Cada Estado parte adoptará las medidas que sean necesarias, de conformidad con los principios de su derecho interno, para garantizar que las entidades o personas perjudicadas como consecuencia de [la utilización de las tecnologías de la información

y las comunicaciones con fines delictivos] [la ciberdelincuencia] tengan derecho a iniciar una acción legal contra los responsables de esos daños y perjuicios a fin de obtener indemnización.

Artículo 55. Medidas para intensificar la 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 los delitos establecidos de conformidad con la presente Convención a:

a) proporcionar información útil a las autoridades competentes con fines investigativos y probatorios sobre cuestiones como:

i) la identidad, la naturaleza, la composición, la estructura, la ubicación o las actividades de las personas que participen en delitos establecidos en virtud de la presente Convención;

ii) los vínculos, incluidos los vínculos internacionales, con otras personas que participen en delitos tipificados con arreglo a la presente Convención;

iii) otros delitos que hayan cometido o puedan cometer las personas que participen en delitos tipificados con arreglo a la presente Convención;

b) prestar ayuda efectiva y concreta a las autoridades competentes que pueda contribuir a privar a las personas involucradas en delitos tipificados con arreglo a la presente Convención de sus recursos o del producto del delito.

2. Cada Estado parte considerará la posibilidad de prever, en los casos apropiados, la mitigación de la pena de las personas acusadas que presten una cooperación sustancial en la investigación o el enjuiciamiento respecto de los delitos comprendidos en 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 preste cooperación sustancial en la investigación o el enjuiciamiento de los delitos tipificados con arreglo a la presente Convención.

4. La protección de esas personas será la prevista en el artículo de la presente Convención relativo a la protección de testigos.

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.