

**MENSAJE DE S.E. LA PRESIDENTA DE
LA REPÚBLICA CON EL QUE INICIA UN
PROYECTO DE ACUERDO QUE APRUEBA EL
CONVENIO SOBRE LA CIBER-
DELINCUENCIA.**

Santiago, 06 de mayo de 2016.-

M E N S A J E N° 050-364/

Honorable Cámara de Diputados:

**A S.E. EL
PRESIDENTE
DE LA H.
CÁMARA DE
DIPUTADOS**

En virtud de mis facultades constitucionales, tengo el honor de someter a vuestra consideración el "Convenio sobre la Ciberdelincuencia", suscrito en Budapest, Hungría, el 23 de noviembre de 2001.

I. ANTECEDENTES

El Convenio sobre la Ciberdelincuencia del Consejo de Europa, conocido como el "Convenio de Budapest", constituye el primer tratado internacional sobre delitos cometidos a través de internet y de otros sistemas informáticos. Fue elaborado por expertos del Consejo de Europa, con ayuda de especialistas de otros países ajenos a la Organización, como Estados Unidos, Canadá y Japón.

El Convenio de Budapest entró en vigor el 1° de julio de 2004 y, a la fecha, ha sido ratificado por cuarenta y siete Estados. Además, cabe señalar que han sido invitados a hacerse Parte del referido Convenio otros Estados no miembros del Consejo de Europa, entre ellos, Argentina, Chile, Costa Rica, Colombia, México y Perú.

El principal objetivo del Convenio es el desarrollo de una política criminal común frente al ciberdelito, mediante la homologación de la legislación penal, sustantiva y procesal, y el establecimiento de un sistema rápido y eficaz de cooperación internacional.

Así, es posible constatar que existen diversos ilícitos asociados al uso de plataformas tecnológicas. Algunos de ellos son exclusivamente del ámbito del ciberespacio, como el sabotaje informático o el acceso indebido a sistemas de información, en tanto otros pueden ser facilitados o tener un alcance mayor gracias a internet, como la estafa, la adquisición o almacenamiento de material pornográfico infantil y la comercialización y producción de éste.

Nuestro país no está ajeno a la ocurrencia de este tipo de criminalidad y, de hecho, contamos desde el año 1993 con una ley que tipifica figuras penales relativas a la informática (ley N° 19.223). A mayor abundamiento, el incremento en el uso de internet, que de acuerdo a la información proporcionada por la Subsecretaría de Telecomunicaciones ha aumentado de 585.489 conexiones fijas en el año 2000 a 2.556.914 en el año 2015, conlleva mayores probabilidades de que ocurran ilícitos de este tipo. Así, por ejemplo, de acuerdo a datos proporcionados por el Ministerio Público, los casos ingresados por sabotaje informático han aumentado de 5 el año 2006 a 770 el año 2014, mientras el espionaje informático aumentó de 1 caso el año 2006 a 206 el año 2014.

No obstante lo anterior, nuestra legislación no tipifica ciertas figuras penales. La adhesión al Convenio de Budapest nos obligaría a considerar un catálogo de delitos más exhaustivo y actualizado. En efecto, dicho instrumento establece que las Partes deberán adoptar en sus legislaciones nacionales determinados tipos penales relativos a violaciones de sistemas informáticos, fraude informático, pornografía infantil e infracción a la propiedad intelectual.

El ciberespacio no reconoce fronteras, permitiendo iniciar en un Estado la ejecución

de una conducta ilícita para generar sus efectos en otro y aprovecharse de las ganancias en un tercero. Todo esto puede ocurrir en forma instantánea, debido a que el desarrollo tecnológico basado en la interconexión global permite lograrlo a bajo costo, con menores riesgos y con altos niveles de eficacia. Por este motivo, para la detección y sanción de estas prácticas ilegales, es imperiosa la asistencia internacional que nos ofrece el Convenio de Budapest, particularmente el sistema de comunicación y asistencia técnica entre países en un formato de veinticuatro horas al día, siete días a la semana.

II. ESTRUCTURA Y CONTENIDO DEL CONVENIO

El Convenio se encuentra estructurado sobre la base de un Preámbulo, en donde se consignan los motivos que tuvieron a las Partes para adoptarlo; y de cuarenta y ocho artículos, donde se despliegan las normas que conforman su cuerpo dispositivo.

En el Preámbulo, los Estados Miembros del Consejo de Europa y los otros Estados firmantes señalan el objetivo del Convenio, cual es llevar a cabo, con prioridad, una política penal común destinada a prevenir la criminalidad en el ciberespacio y, en particular, hacerlo mediante la adopción de una legislación apropiada y una mejora de la cooperación internacional.

Los cuarenta y ocho artículos, por su parte, se contienen en cuatro Capítulos que, a su vez, se dividen en Secciones, y estas últimas en Títulos. En ellos se tratan los temas que se indican a continuación.

1. Capítulo I: Terminología

El Artículo 1 del Convenio, único artículo del primer Capítulo, precisa una serie de definiciones necesarias para la correcta aplicación del Convenio, tales como, "sistema informático", "datos informáticos", "proveedor de servicios", y "datos relativos al tráfico".

2. Capítulo II: Medidas que deberán adoptarse a nivel nacional

Este Capítulo está compuesto de tres Secciones. Las dos primeras cuentan con cinco Títulos cada una, mientras la tercera no tiene ninguno.

a. Sección 1: Derecho penal sustantivo

El **Título 1** de esta Sección se refiere a los delitos contra la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos.

En este contexto, el Convenio consagra la obligación de los Estados Parte de adoptar las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las siguientes conductas:

i. Acceso ilícito (Artículo 2): El acceso deliberado e ilegítimo a todo o parte de un sistema informático. Además, se faculta a las Partes para exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación a un sistema informático conectado a otro sistema informático.

ii. Interceptación ilícita (Artículo 3): 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. Asimismo, se faculta a los Estados Parte a exigir que el delito se cometa con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

iii. Ataques a la integridad de los datos (Artículo 4): Todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o

suprima datos informáticos. Sin perjuicio de ello, se faculta a las Partes a reservarse el derecho a exigir que los referidos actos ocasionen daños que puedan calificarse de graves.

iv. Ataques a la integridad del sistema (Artículo 5): 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.

v. Abuso de los dispositivos (Artículo 6): La comisión deliberada e ilegítima de los siguientes actos:

- La producción, venta, obtención para su utilización, importación, difusión u otras formas de puesta a disposición de: (a) cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos previstos en los Artículos 2 a 5 del Convenio; (b) 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 señalados Artículos 2 a 5; y

- La posesión de alguno de los elementos señalados precedentemente con intención de que sean utilizados para cometer cualquiera de los delitos previstos en los Artículos 2 a 5 del Convenio. Se faculta, además, a las Partes a exigir en su derecho interno un determinado número de dichos elementos para que se considere que existe responsabilidad penal.

Se agrega, también, que el Artículo 6 del Convenio no se interpretará para que imponga responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, difusión o cualquier otra forma de puesta a disposición mencionada en el párrafo precedente no tenga por objeto la

comisión de uno de los delitos previstos en los Artículos 2 a 5 del mismo.

Finalmente, se faculta a las Partes para que puedan realizar una reserva en relación al párrafo 1 del Artículo 6 del Convenio, cumpliendo determinados requisitos.

El **Título 2** de esta Sección, por su parte, se refiere a los delitos informáticos.

Así, se dispone que cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las siguientes conductas:

i. Falsificación informática (Artículo 7): 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. Con todo, las Partes podrán exigir que exista una intención dolosa o delictiva similar para que se considere que existe responsabilidad penal.

ii. Fraude informático (Artículo 8): Los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante la introducción, alteración, borrado o supresión de datos informáticos; y cualquier interferencia en el funcionamiento de un sistema informático, realizados con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.

El **Título 3** de esta Sección, a su vez, trata sobre los delitos relacionados con el contenido. En este marco, se refiere a los delitos relacionados con la pornografía infantil, enumerándose, en el párrafo 1 del Artículo 9 del Convenio, los actos que cometidos, deliberada e ilegítimamente, deberán ser tipificados por las Partes como delito en su derecho interno, para lo que deberán adoptar las medidas legislativas y de otro tipo que resulten necesarias. Se precisa, además, qué comprende la expresión

"pornografía infantil", qué se entiende por "menor" y la facultad de las Partes a reservarse el derecho a no aplicar, en todo o parte, los apartados d) y e) del párrafo 1 y los apartados b) y c) del párrafo 2, todos del Artículo 9.

Asimismo, el **Título 4** de esta Sección trata sobre los delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines. Así, el Artículo 10 del Convenio indica que cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de la propiedad intelectual que defina su legislación, conforme a las obligaciones que haya asumido en aplicación del Acta de París de 24 de julio de 1971, por la que se revisó el Convenio de Berna para la protección de 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 conferido por dichos Convenios, cuando tales actos sean cometidos deliberadamente, a escala comercial y a través de un sistema informático.

Igualmente, se prevé que cada Parte adoptará las medidas legislativas o de otro tipo que se estimen necesarias para tipificar como delito en su derecho interno las infracciones de los derechos afines definidas en su legislación, de conformidad a las obligaciones que haya asumido por 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 Convenios, cuando tales actos sean cometidos deliberadamente, a escala comercial y a través de un sistema informático.

Finalmente, el Artículo 10 establece que las Partes, en circunstancias bien delimitadas, podrán reservarse el derecho de no imponer responsabilidad penal en aplicación de los dos párrafos precedentes, siempre que se disponga de otros recursos efectivos y que dicha reserva no vulnere las obligaciones internacionales que incumban al Estado por aplicación de los instrumentos internacionales mencionados.

Por último, el **Título 5** de esta Sección se refiere a otras formas de responsabilidad y de sanción, cuales son las siguientes:

i. Tentativa y complicidad: El Artículo 11 norma que cada Parte adoptará las medidas legislativas y de otro tipo que se estimen necesarias para tipificar como delito en su derecho interno cualquier complicidad deliberada con vistas a la comisión de alguno de los delitos previstos en aplicación de los Artículos 2 a 10 del Convenio, con la intención de que dicho delito sea cometido.

Asimismo, se indica que cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno toda tentativa deliberada de cometer alguno de los delitos previstos en aplicación de los Artículos 3 a 5, 7, 8, y 9.1 a) y 9.1.c) del Convenio.

No obstante, se establece la facultad de los Estados Partes de reservarse el derecho de no aplicar, en todo o en parte, el párrafo precedente.

ii. Responsabilidad de las personas jurídicas: El Artículo 12 dispone que cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que pueda exigirse responsabilidad a las personas jurídicas por los delitos previstos en aplicación del Convenio, estableciendo los casos, y para garantizar que pueda exigirse responsabilidad a una persona jurídica cuando la ausencia de vigilancia o de control por parte de una persona física haya permitido la comisión de un delito.

Finalmente, se señala el tipo de responsabilidad de la persona jurídica y se consigna que dicha responsabilidad se establecerá sin perjuicio de la responsabilidad penal de las personas naturales que hayan cometido la infracción.

iii. Sanciones y medidas: En relación a las sanciones y medidas establecidas en el Convenio, el Artículo 13 señala que cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que los delitos previstos en aplicación de los Artículos 2 a 11 del Convenio estén sujetos a sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad. Por su parte, en relación a las personas jurídicas que hayan sido consideradas responsables de conformidad con el Artículo 12, las Partes garantizarán la imposición de sanciones o medidas penales o no penales efectivas, proporcionadas y disuasorias, incluidas las sanciones pecuniarias.

b. Sección 2: Derecho procesal

El **Título 1** de esta Sección trata sobre disposiciones comunes.

De este modo, se refiere al ámbito de aplicación de las disposiciones sobre procedimiento. En este contexto, el Artículo 14 indica que cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para establecer los poderes y procedimientos previstos en esta sección a los efectos de investigación o de procedimientos penales específicos.

Luego, salvo que se establezca lo contrario en el Artículo 21, relativo a la interceptación de datos relativos al contenido, cada Parte aplicará los poderes y procedimientos mencionados en el párrafo 1 del Artículo 14 a los delitos previstos en aplicación de los Artículos 2 a 11 del Convenio; a cualquier otro delito cometido a través de un sistema informático; y a la obtención de pruebas electrónicas de cualquier delito.

Además, se faculta a las Partes a reservarse el derecho de aplicar las medidas mencionadas en el Artículo 20, referida a la recogida en tiempo real de datos informáticos, a los delitos o categorías de delitos especificados en su reserva, siempre que el repertorio de dichos delitos o categorías de delitos no sea más reducido que el de los delitos a que dicha Parte aplique las medidas mencionadas en el Artículo 21. Las Partes, asimismo, tratarán de limitar tal reserva de modo que sea posible la más amplia aplicación de la medida contemplada en el Artículo 20.

Sin perjuicio de lo anterior, se establece que cuando una Parte, en razón de las restricciones impuestas por su legislación vigente en el momento de la adopción del Convenio, no pueda aplicar las medidas previstas en los Artículos 20 y 21 a las comunicaciones transmitidas dentro de un sistema informático de un proveedor de servicios que se haya puesto en funcionamiento para un grupo restringido de usuarios, que no emplee las redes públicas de telecomunicación y que no esté conectado a otro sistema informático, público o privado, la referida Parte podrá reservarse el derecho a no aplicar dichas medidas a esas comunicaciones, buscando siempre limitar tal reserva de modo que se permita la aplicación lo más amplia posible de las medidas mencionadas en los Artículos 20 y 21.

Asimismo, este Título trata las condiciones y salvaguardias. Así, el Artículo 15 indica que cada Parte se asegurará de que la instauración, ejecución y aplicación de los poderes y procedimientos previstos en la Sección 2 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 derivados de las obligaciones que haya asumido cada Parte en aplicación del Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) u otros instrumentos internacionales relativos a los derechos humanos, y que deberá

integrar el principio de proporcionalidad. Además, cuando proceda, en atención a la naturaleza del procedimiento o del poder de que se trate, dichas condiciones y salvaguardias incluirán una supervisión judicial u otra forma de supervisión independiente, los motivos que justifiquen su aplicación, así como la limitación del ámbito de aplicación y la duración de dicho poder o procedimiento.

Finalmente, se establece que cada Parte deberá examinar, siempre que sea conforme con el interés público, y en particular con la buena administración de justicia, los efectos de los poderes y procedimientos establecidos en esta Sección sobre los derechos, responsabilidades e intereses legítimos de terceros.

El **Título 2** de esta Sección, por su parte, se refiere a la conservación rápida de datos informáticos almacenados.

De esta forma, el Artículo 16 contempla que cada Parte adoptará las medidas legislativas y de otro tipo que se estimen necesarias para permitir a sus autoridades competentes ordenar o imponer de otro modo la conservación rápida de datos electrónicos específicos, incluidos los datos de tráfico, almacenados a través de un sistema informático, especialmente cuando hayan razones para creer que dichos datos son particularmente susceptibles de pérdida o de modificación. Igualmente, cuando una Parte aplique lo anterior por medio de una orden impartida a una persona que conserve determinados datos almacenados que se encuentren en poder o bajo el control de esa persona, deberá adoptar las medidas legislativas y de otro tipo que resulten necesarias para obligar a dicha persona a conservar y proteger la integridad de los datos durante el tiempo necesario, hasta un máximo de noventa días, con el objeto de permitir a las autoridades competentes obtener su revelación.

Adicionalmente, se establece que cada Parte adoptará las medidas legislativas y de otro tipo que se estimen necesarias para

obligar a la persona que custodia los datos o a otra persona encargada de conservarlos a mantener en secreto la ejecución de dichos procedimientos durante el tiempo previsto por el ordenamiento jurídico nacional.

Finaliza el Artículo 16 señalando que tanto los poderes como los procedimientos mencionados en él quedarán sometidos a las medidas y garantías preceptuadas en los Artículos 14 y 15.

Por su parte, el Artículo 17 aborda la conservación y divulgación de los datos de tráfico, estatuyendo que a fin de asegurar la conservación de éstos, en aplicación del Artículo 16, cada Parte adoptará las medidas legislativas y de otro tipo que se estimen necesarias para garantizar la conservación rápida de los datos relativos al tráfico, ya sean uno o más prestadores de servicio que hayan participado en la transmisión de dicha comunicación; y asegurar la revelación rápida a la autoridad competente de la Parte, o a una persona designada por dicha autoridad, de un volumen de datos de tráfico suficiente para permitir la identificación de los prestadores de servicio y de la vía por la que la comunicación se ha transmitido.

Finalmente se indica que tanto los poderes como los procedimientos mencionados en el Artículo 17 quedarán sujetos a las medidas y garantías establecidas en los Artículos 14 y 15.

El **Título 3** de esta Sección regula el orden de presentación. De este modo, el Artículo 18 del Convenio consigna un mandato de comunicación a las Partes indicando que éstas adoptarán las medidas legislativas y de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para ordenar a una persona presente en su territorio que comunique determinados datos informáticos que obren en su poder o bajo su control, almacenados en un sistema informático o en un dispositivo de almacenamiento informático; y/o ordenar a un proveedor que ofrezca sus servicios en el territorio de dicha Parte, que comunique los datos en su poder o bajo su control relativos a los

abonados en relación a tales servicios, entendiéndose por "datos relativos a los abonados" cualquier información, en forma de datos informáticos o de cualquier otro modo, que posea un proveedor de servicio y que se refiera a los abonados de sus servicios, diferentes de los datos relativos al tráfico o al contenido y que permitan determinar:

- El tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el tiempo del servicio;

- La identidad, la dirección postal o situación geográfica y el número de teléfono del abonado o cualquier otro número de acceso y los datos relativos a la facturación y el pago, disponibles por razón de un contrato o de un acuerdo de prestación de servicio; y

- Cualquier otra información relativa al lugar donde se ubican los equipos de comunicación, disponible por razón de un contrato o de un acuerdo de prestación de servicios.

Ahora, en relación a los poderes y procedimientos mencionados en el indicado Artículo 18, se indica que éstos quedarán sometidos a los Artículos 14 y 15.

El **Título 4** de esta Sección, a su vez, trata sobre el registro y confiscación de datos informáticos almacenados.

Así, el Artículo 19 preceptúa que cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a registrar o acceder de un modo similar a un sistema informático o a una parte del mismo, así como a los datos informáticos que están almacenados; y a todo dispositivo de almacenamiento que permita contener datos informáticos en su territorio.

Igualmente, se agrega que cada Parte adoptará las medidas legislativas y de otro tipo que se estimen necesarias para asegurarse de que cuando, de conformidad con el apartado 1. a) del señalado artículo, sus autoridades registren o tengan acceso de un modo similar a

un sistema informático específico o a una parte del mismo y tengan motivos para creer que los datos buscados se hallan almacenados en otro sistema informático o en una parte del mismo situado en su territorio, y que dichos datos son igualmente accesibles a partir del sistema inicial o están disponibles a través de ese primer sistema, puedan extender rápidamente el registro o el acceso de un modo similar al otro sistema.

Asimismo, cada Parte adoptará las medidas legislativas y de otro tipo que se estimen necesarias para facultar a sus autoridades competentes a confiscar u obtener de un modo similar los datos informáticos cuyo acceso haya sido realizado en aplicación de los párrafos precedentes. Estas medidas incluirán las siguientes prerrogativas: a) confiscar u obtener de un modo similar un sistema informático o una parte del mismo o un dispositivo de almacenamiento informático; b) realizar y conservar una copia de esos datos informáticos; c) preservar la integridad de los datos informáticos almacenados pertinentes; y d) hacer inaccesibles o suprimir los datos informáticos del sistema informático consultado.

Además, se indica que cada Parte adoptará las medidas legislativas y de otro tipo que se estimen necesarias a fin de facultar a sus autoridades competentes a ordenar a toda persona que conozca el funcionamiento de un sistema informático o las medidas aplicadas para proteger los datos informáticos que contiene, que proporcione toda la información necesaria, dentro de lo razonable, para permitir la aplicación de las medidas previstas en los párrafos 1 y 2 del Artículo 19.

Finalmente, en relación al límite al ejercicio de los poderes y procedimientos mencionados en el indicado Artículo 19, éstos quedarán sometidos a lo establecido en los Artículos 14 y 15.

Por último, el **Título 5** de esta Sección se refiere a la obtención en tiempo real de datos informáticos.

De esta forma, el Artículo 20 señala que cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias a fin de facultar a sus autoridades competentes para obtener o grabar con medios técnicos existentes en su territorio y obligar a cualquier proveedor de servicios, en la medida de sus capacidades técnicas, a obtener o grabar con medios técnicos existentes en su territorio o a ofrecer a las autoridades competentes su colaboración y su asistencia para obtener o grabar, en tiempo real, los datos relativos al tráfico asociados a comunicaciones específicas transmitidas en su territorio a través de un sistema informático.

Ahora, para el caso en que un Estado, en razón de los principios establecidos en su ordenamiento jurídico interno, no pueda adoptar las medidas conducentes a obtener o grabar con medios técnicos existentes en su territorio, podrá, en su lugar, adoptar las medidas legislativas y de otro tipo que estime necesarias para asegurar la obtención o la grabación en tiempo real de los datos relativos al tráfico asociados a comunicaciones específicas transmitidas en su territorio mediante la aplicación de medios técnicos existentes en ese territorio.

Adicionalmente, se explicita que cada Parte adoptará las medidas legislativas y de otro tipo que se estimen necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se haya ejercido cualquiera de los poderes previstos en el Artículo 20, así como cualquier información al respecto.

Finalmente, se prescribe que tanto los poderes como los procedimientos mencionados en el Artículo 20 deben quedar sometidos a los Artículos 14 y 15.

En relación a la interceptación de datos relativos al contenido, el Artículo 21 establece que cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes respecto a un repertorio de delitos graves que deberá definirse en su derecho interno para obtener o grabar con

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

Con todo, cuando un Estado, en razón de los principios establecidos en su ordenamiento jurídico interno, no pueda adoptar las medidas conducentes a obtener o grabar con medios técnicos existentes en su territorio, podrá, en su lugar, adoptar las medidas legislativas y de otro tipo que estime necesarias para asegurar la obtención o la grabación en tiempo real de los datos relativos al contenido de comunicaciones específicas transmitidas en su territorio mediante la aplicación de medios técnicos existentes en ese territorio.

Por su parte, al igual que en el Artículo 20, se establece que cada Parte adoptará las medidas legislativas y de otro tipo que se estimen necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se haya ejercido cualquiera de los poderes previstos en dicho Artículo, así como cualquier información al respecto.

En relación a los poderes y procedimientos mencionados en el Artículo 21, cabe precisar que ellos quedarán limitados por la regulación indicada en los Artículos 14 y 15.

c. Sección 3: Jurisdicción

El Artículo 22 indica que cada Parte adoptará las medidas legislativas y de otro tipo que se estimen necesarias para afirmar su jurisdicción respecto de cualquier delito previsto de conformidad con los Artículos 2 a 11 del Convenio, cuando el delito se haya cometido:

i. En su territorio; o

ii. A bordo de un buque que enarbole su pabellón ; o

iii. A bordo de una aeronave matriculada según sus leyes; o

iv. Por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar que se cometió o si ningún Estado tiene competencia territorial respecto del mismo.

Ahora bien, las Partes podrán reservarse el derecho de no aplicar, o de aplicar sólo en ciertos casos o condiciones, las normas sobre jurisdicción establecidas en los apartados 1.b) a 1.d) del Artículo 22 o en cualquier parte de dichos apartados.

Adicionalmente, se establece que las Partes adoptarán las medidas que se estimen necesarias para afirmar su jurisdicción respecto de cualquier delito previsto en el Artículo 24, párrafo 1, referido a la extradición por los delitos de los Artículos 2 a 11, inclusive, del Convenio, cuando el presunto autor del mismo se halle en su territorio y no pueda ser extraditado a otra Parte por razón únicamente de la nacionalidad, previa demanda de extradición.

Además, se explicita que el Convenio no excluye ninguna jurisdicción penal ejercida por una Parte de conformidad con su derecho interno.

Finalmente, para el caso en que varias Partes reivindiquen su jurisdicción respecto de un presunto delito contemplado en el Convenio, se establece que las Partes interesadas celebrarán consultas, cuando ello sea oportuno, a fin de decidir cuál jurisdicción es más adecuada para entablar la acción penal.

3. Capítulo III: Cooperación internacional

Este Capítulo está dividido en dos Secciones, de cuatro Títulos el primero y tres el segundo.

a. Sección 1: Principios generales

El **Título 1** de esta Sección se refiere a los principios generales relativos a la cooperación internacional.

El Artículo 23 señala que las Partes cooperarán entre sí en la mayor medida posible de conformidad con lo dispuesto en el Capítulo III, en aplicación de los instrumentos internacionales sobre cooperación internacional en materia penal, de los acuerdos basados en legislación uniforme o recíproca y en su propio derecho nacional, en relación con las investigaciones o los procedimientos concernientes a los delitos relacionados con sistemas y datos informáticos o para obtener pruebas en formato electrónico de los delitos.

El **Título 2** de esta Sección, por su parte, trata los principios relativos a la extradición.

Así, el Artículo 24 se aplica a la extradición entre las Partes por los delitos definidos de conformidad con los Artículos 2 a 11 del Convenio, siempre que sean castigados por la legislación de las dos Partes implicadas con una pena privativa de libertad de una duración mínima de un año, o con una pena más grave.

Cuando se aplique una pena mínima diferente, en virtud de un tratado de extradición aplicable entre dos o más Partes, incluido el Convenio Europeo de Extradición (STE n° 24) o de un acuerdo basado en la legislación uniforme o recíproca, se aplicará la pena mínima prevista en dicho tratado o acuerdo. Se considerará que los delitos descritos en el párrafo 1 del Artículo 24 están incluidos entre los delitos que dan lugar a la extradición como asimismo las Partes se comprometen a incluirlos en los tratados que puedan concluir.

Ahora bien, si una Parte condiciona la extradición a la existencia de un tratado y recibe una demanda de extradición de una Parte con la que no lo ha concluido, podrá considerar el Convenio como fundamento jurídico suficiente para conceder la

extradición por alguno de los delitos previstos en los Artículos 2 a 11 del mismo. En el caso en que las Partes no condicionen la extradición a la existencia de un tratado, reconocerán los delitos mencionados en el párrafo 1 del Artículo 24 como delitos que pueden dar lugar a la extradición entre ellas.

La extradición quedará sometida a las condiciones establecidas en el derecho interno de la Parte requerida o en los tratados de extradición vigentes, quedando asimismo sometidos a estos instrumentos jurídicos los motivos por los que la Parte requerida puede denegar la extradición.

Se señala también que en caso de denegarse la extradición por un delito comprendido en el párrafo 1 del Artículo 24 en razón de la nacionalidad de la persona reclamada o porque la Parte requerida se considera competente, ésta deberá someter el asunto a sus autoridades competentes a efectos de la acción penal pertinente.

Finalmente se indica que las Partes deberán comunicar al Secretario General del Consejo de Europa el nombre y dirección de cada autoridad responsable del envío y de la recepción de las demandas de extradición o de detención provisional, en ausencia de tratado.

El **Título 3** de esta Sección, a su vez, se refiere a los principios generales relativos a la asistencia mutua.

En este contexto, el Artículo 25 trata de la ayuda entre las Partes a efectos de las investigaciones o de los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o con el fin de obtener pruebas en formatos electrónicos de un delito, de igual forma señala que cada Parte adoptará las medidas legislativas y de otro tipo que estimen necesarias para dar cumplimiento a las obligaciones establecidas en los Artículos 27 a 35.

También se establece que las Partes podrán, en caso de urgencia, formular una solicitud de asistencia mutua o realizar las comunicaciones relativas a la misma, a través de medios de comunicación rápidos, como el fax

o el correo electrónico, procurando que esos medios ofrezcan las condiciones suficientes de seguridad y de autenticación (encriptándose si fuera necesario) y con confirmación posterior de la misma si el Estado requerido lo exigiera.

Asimismo, se preceptúa que, salvo disposición en contrario expresamente prevista en el Capítulo III, la asistencia estará sometida a las condiciones fijadas en el derecho interno de la Parte requerida o en los tratados de asistencia aplicables, incluidos los motivos por los que el Estado requerido puede negarse a colaborar, no obstante, el Estado requerido no ejercerá dicho derecho en relación a las infracciones previstas en los Artículos 2 a 11, alegando que la solicitud se refiere a un delito que considera de carácter fiscal.

Finalmente, se explicita que el Estado requerido estará autorizado a supeditar la colaboración a la exigencia de doble incriminación.

Por su parte, el Artículo 26 prescribe que las Partes podrán, dentro de los límites de su derecho interno y sin que exista demanda previa, comunicar a otra Parte la información obtenida en el marco de sus propias investigaciones si considera que puede ayudar a la Parte destinataria a iniciar o a concluir investigaciones o procedimientos en relación con los delitos previstos de conformidad con el Convenio o cuando dicha información pueda conducir a una petición de cooperación de dicha Parte en virtud del Capítulo III. Asimismo, se indica que antes de comunicar dicha información, la Parte que la proporciona podrá solicitar que la información sea tratada de forma confidencial o que sólo sea utilizada bajo ciertas circunstancias. Luego, si la Parte destinataria no pudiera acatar las condiciones impuestas, deberá informar a la otra Parte, quien habrá de decidir si proporciona o no la información.

Por último, el **Título 4** de esta Sección trata sobre los procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables.

En este marco, el Artículo 27 regula el procedimiento relativo a las solicitudes de colaboración en ausencia de acuerdos internacionales aplicables, señalando que en tal caso se aplicarán las disposiciones de los párrafos 2 a 9 de dicho artículo.

Cabe destacar que, en virtud de esta disposición, se deberá comunicar al Secretario General del Consejo de Europa la autoridad central encargada de enviar las solicitudes de asistencia mutua o de responder las mismas, de ejecutarlas o de remitirlas a las autoridades competentes para su ejecución.

Asimismo, el Artículo 28 contempla la situación de inexistencia de tratados o acuerdos en vigor de asistencia basados en la legislación uniforme o recíproca, disponiendo que será aplicable dicho artículo. Así, el Estado requerido podrá supeditar la comunicación de la información o del material requerido en la solicitud al cumplimiento de las siguientes condiciones: a) que se mantenga la confidencialidad sobre las mismas; o b) que éstas no sean utilizadas en investigaciones o procedimientos diversos a los establecidos en la solicitud.

Igualmente, se establece que si la Parte requirente no pudiera satisfacer alguna de las referidas condiciones informará a la Parte requerida, la cual decidirá si la información debe ser proporcionada.

b. Sección 2: Disposiciones específicas

El **Título 1** de esta Sección se refiere a la asistencia mutua en materia de medidas provisionales.

De este modo, el Artículo 29 señala que una Parte podrá solicitar a la otra Parte que ordene o imponga de otro modo la conservación rápida de datos almacenados por medios de sistemas informáticos que se encuentren en el territorio de esa otra Parte, y en relación con los cuales la Parte requirente tenga intención de presentar una solicitud de asistencia mutua con vistas al registro o al acceso por un medio similar, la confiscación o la obtención por un medio similar, o a la revelación de dichos actos.

Agrega esta disposición los requisitos de dicha solicitud de conservación y consigna la obligación de la Parte requerida de adoptar las medidas necesarias para proceder sin demora a la conservación de los datos solicitados, de conformidad a su derecho interno.

Estatuye, además, que para responder solicitudes de este tipo no se requiere la doble tipificación penal para proceder a la conservación salvo cuando una Parte la exige como condición para atender a una solicitud de asistencia mutua con vistas al registro o al acceso por una medio similar, a la confiscación o a la obtención por un medio similar o a la revelación de datos almacenados en relación con delitos diferentes de los previstos de conformidad con los Artículos 2 a 11 del Convenio, la cual podrá reservarse el derecho a denegar la solicitud de conservación en virtud del Artículo 29 en caso que tenga motivos para creer que, en el momento de la revelación de los datos, no se cumplirá la condición de la doble tipificación penal.

Sin perjuicio de lo anterior, se establece que las solicitudes de conservación sólo podrán ser denegadas si la solicitud se refiere a un delito que la Parte requerida considera de naturaleza política o vinculada a un delito de carácter político; o la Parte requerida estima que la ejecución de la solicitud podría atentar contra su soberanía, su seguridad, orden público u otros intereses esenciales.

Adicionalmente, se señala que cuando la Parte requerida considere que la simple conservación por sí sola de los datos no bastará para garantizar la disponibilidad futura, o que pondrá en peligro la confidencialidad de la investigación de la Parte requirente, o causará cualquier otro perjuicio a la misma, informará de ello rápidamente a la Parte requirente, quien determinará a continuación la conveniencia, no obstante, de dar curso a la solicitud.

Finalmente, se indica que las medidas de conservación adoptadas en respuesta a solicitudes de conservación serán válidas por

un periodo mínimo de 60 días, para permitir, dentro de ese plazo, a la Parte requirente formular una solicitud de asistencia para registrar o acceder de otro modo, confiscar u obtener por otro medio similar, la revelación de dichos datos.

El Artículo 30, por su parte, prevé que si al ejecutar una solicitud formulada de conformidad al Artículo 29 para la conservación de datos relativos de tráfico de una determinada comunicación la Parte requerida descubriera que un proveedor de servicios de otro Estado ha participado en la transmisión de dicha comunicación, dicha Parte revelará rápidamente a la Parte requirente un volumen suficiente de datos relativos al tráfico para que pueda identificarse al proveedor de servicios, así como la vía por la que la comunicación ha sido transmitida.

Asimismo, establece en qué casos se puede denegar la revelación de datos según el párrafo anterior.

El **Título 2** de esta Sección, a su vez, regula la asistencia mutua en relación con los poderes de investigación.

El Artículo 31 faculta a una Parte a solicitar a otra Parte el registro o el acceso de un modo similar, la confiscación o la obtención de un modo similar o la revelación de datos almacenados por medio de un sistema informático que se encuentre en el territorio de esa otra Parte, incluidos los datos conservados de conformidad con el Artículo 29. La Parte requerida responderá a la solicitud aplicando los instrumentos internacionales, acuerdos y legislación mencionados en el Artículo 23, así como de conformidad con las disposiciones pertinentes del presente Capítulo. Se consigna en qué casos la solicitud se deberá responder rápidamente.

El Artículo 32, a su vez, establece los casos en los cuales una Parte podrá, sin autorización de otra acceder a los datos informáticos almacenados de libre acceso al público (fuentes abiertas), independiente de su localización geográfica; o acceder a, o recibir a través de un sistema informático

situado en su territorio, los datos informáticos almacenados situados en otro Estado, si dicha Parte obtiene el consentimiento lícito y voluntario de la persona autorizada para divulgarlos a través de ese sistema informático.

Igualmente, el Artículo 33 prescribe que las Partes se prestarán asistencia mutua para la obtención en tiempo real de datos de tráfico asociados a comunicaciones concretas transmitidas en su territorio por medio de un sistema informático, la cual se someterá a las condiciones y procedimiento previstos en el derecho interno. Además, cada Parte colaborará respecto a aquellos delitos para los cuales sea posible la obtención en tiempo real de datos relativos al tráfico en situaciones análogas en base a su derecho interno.

Asimismo, el Artículo 34 dispone que las Partes se presten asistencia mutua, en la medida en que lo permitan sus tratados y leyes internas aplicables, para la obtención o el registro en tiempo real de datos relativos al contenido de comunicaciones específicas transmitidas por medio de un sistema informático.

Finalmente, el **Título 3** de esta Sección se refiere a la Red 24/7.

Conforme lo señalado en el Artículo 35, las Partes deberán fijar un punto de contacto localizable las 24 horas del día, y los siete días de la semana, con el fin de asegurar la asistencia inmediata en la investigación de delitos vinculados a sistemas y datos informáticos, o para obtener las pruebas en formato electrónico de un delito. De igual forma señala qué comprenderá la referida asistencia.

4. Capítulo IV: Cláusulas finales

Concluye el texto del Convenio con las cláusulas finales que son de uso corriente en esta clase de instrumentos internacionales, regulando desde el Artículo 36 al 48, respectivamente, las siguientes materias: la firma y entrada en vigor, la adhesión, la aplicación territorial, los efectos, las

declaraciones, la cláusula federal, las reservas, el mantenimiento y retiro de las reservas, las enmiendas, la solución de controversias, las consultas entre las Partes, la denuncia y la notificación que efectuará el Secretario General del Consejo de Europa.

III. DECLARACIONES Y RESERVAS AL CONVENIO

De conformidad a lo previsto en el articulado del Convenio, el Ejecutivo comunica su decisión de formular las siguientes declaraciones y reservas al momento de depositar el instrumento de adhesión al referido Convenio:

1. Declaraciones

a. "La República de Chile declara que exigirá una intención delictiva determinada en el sujeto activo para penar las acciones descritas en los Artículos 2 y 3 del Convenio sobre la Ciberdelincuencia, conforme lo requiere el Artículo 2 de la Ley N° 19.223 sobre delitos informáticos".

b. "La República de Chile declara que exigirá un ánimo fraudulento que produzca un perjuicio a terceros para penar las acciones descritas en el Artículo 7 del Convenio sobre la Ciberdelincuencia, conforme lo requiere el Artículo 197 del Código Penal".

2. Reservas

a. "La República de Chile expresa, de conformidad al Artículo 4, párrafo 2, del Convenio sobre la Ciberdelincuencia, que tipificará como delitos en su derecho interno todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos, siempre que dicho acto produzca daños graves".

b. "La República de Chile expresa, de conformidad al Artículo 6, párrafo 3 del Convenio sobre la Ciberdelincuencia, que no aplicará el párrafo 1 del mismo Artículo, en la medida que ello no afecte la venta, distribución o cualesquiera otras formas de

puesta a disposición de los elementos mencionados en el inciso 1 a) ii) del citado Artículo 6".

c. "La República de Chile expresa, de conformidad al Artículo 9, párrafo 4, del Convenio sobre la Ciberdelincuencia, que no aplicará los apartados b) y c) del párrafo 2 del mismo Artículo".

d. "La República de Chile expresa, de conformidad al Artículo 22, párrafo 2, del Convenio sobre la Ciberdelincuencia, que no aplicará las normas sobre jurisdicción establecidas en el apartado 1 d. del mismo Artículo".

e. "La República de Chile se reserva, en relación con el Artículo 29, párrafo 4, del Convenio sobre la Ciberdelincuencia, el derecho a denegar la solicitud de asistencia internacional en caso de la que la conducta perseguida no esté tipificada en Chile al momento del requerimiento".

En consecuencia, tengo el honor de someter a vuestra consideración, el siguiente

P R O Y E C T O D E A C U E R D O :

"ARTÍCULO ÚNICO.- Apruébase el "Convenio sobre la Ciberdelincuencia", suscrito en Budapest, Hungría, el 23 de noviembre de 2001.".

Dios guarde a V.E.,

MICHELLE BACHELET JERIA
Presidenta de la República

JORGE BURGOS VARELA
Ministro del Interior
y Seguridad Pública

HERALDO MUÑOZ VALENZUELA
Ministro de Relaciones Exteriores

JAVIERA BLANCO SUÁREZ
Ministra de Justicia y
Derechos Humanos



Serie de Tratados Europeos- n°185

**CONVENIO
SOBRE LA CIBERDELINCUENCIA**

Budapest, 23.XI.2001

Preámbulo

Los Estados miembros del Consejo de Europa y los demás Estados signatarios del presente Convenio,

Considerando que el objetivo del Consejo de Europa es lograr una unión más estrecha entre sus miembros;

Reconociendo el interés de intensificar la cooperación con los otros Estados Partes en el presente Convenio;

Convencidos de la necesidad de aplicar, con carácter prioritario, una política penal común con objeto de proteger a la sociedad frente a la ciberdelincuencia, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional;

Conscientes de los profundos cambios provocados por la digitalización, la convergencia y la globalización continuas de las redes informáticas;

Preocupados por el riesgo de que las redes informáticas y la información electrónica sean utilizadas igualmente para cometer delitos y de que las pruebas relativas a dichos delitos sean almacenadas y transmitidas por medio de dichas redes;

Reconociendo la necesidad de cooperación entre los Estados y el sector privado en la lucha contra la ciberdelincuencia, así como la necesidad de proteger los intereses legítimos en la utilización y el desarrollo de las tecnologías de la información;

Estimando que la lucha efectiva contra la ciberdelincuencia requiere una cooperación internacional reforzada, rápida y eficaz en materia penal;

Convencidos de que el presente Convenio es necesario para prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, garantizando la tipificación como delito de dichos actos, tal como se definen en el presente Convenio, y la asunción de poderes suficientes para luchar eficazmente contra dichos delitos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones materiales que permitan una cooperación internacional rápida y fiable;

Teniendo presente la necesidad de garantizar el debido equilibrio entre los intereses de la acción penal y el respeto de los derechos humanos fundamentales consagrados en el Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) y otros tratados internacionales aplicables en materia de derechos humanos, que reafirman el derecho a defender la propia opinión sin interferencia, el derecho a la libertad de expresión, incluida la libertad de buscar, obtener y comunicar información e ideas de toda índole, sin consideración de fronteras, así como el respeto de la vida privada;

Conscientes igualmente del derecho a la protección de los datos personales, tal como se define, por ejemplo, en el Convenio de 1981 del Consejo de Europa para la protección de las personas con respecto al tratamiento informatizado de datos personales;

Teniendo presentes la Convención sobre los Derechos del Niño de las Naciones Unidas (1989) y el Convenio sobre las peores formas de trabajo infantil de la Organización Internacional del Trabajo (1999);

Teniendo en cuenta los convenios existentes del Consejo de Europa sobre cooperación en materia penal, así como otros tratados similares celebrados entre los Estados miembros del Consejo de Europa y otros Estados, y subrayando que el objeto del presente Convenio es completar dichos Convenios con el fin de incrementar la eficacia de las investigaciones y procedimientos penales relativos a los delitos relacionados con sistemas y datos informáticos, así como permitir la obtención de pruebas electrónicas de los delitos;

Congratulándose de las recientes iniciativas destinadas a mejorar el entendimiento y la cooperación internacionales en la lucha contra la delincuencia cibernética, y en particular las acciones organizadas por las Naciones Unidas, la OCDE, la Unión Europea y el G8;

Recordando las Recomendaciones del Comité de Ministros nº R (85) 10 relativa a la aplicación práctica del Convenio Europeo de Asistencia Judicial en Materia Penal en relación con las comisiones rogatorias para la vigilancia de las telecomunicaciones, nº R (88) 2 sobre medidas encaminadas a luchar contra la piratería en materia de propiedad intelectual y derechos afines, nº R (87) 15 relativa a la regulación de la utilización de datos de personales por la policía, nº R (95) 4 sobre la protección de los datos personales en el ámbito de los servicios de telecomunicaciones, con especial referencia a los servicios telefónicos, nº R (89) 9 sobre la delincuencia relacionada con la informática, que ofrece a los legisladores nacionales directrices para definir ciertos delitos informáticos, y nº R (95) 13 relativa a los problemas de procedimiento penal vinculados a la tecnología de la información;

Teniendo presente la Resolución nº 1, adoptada por los Ministros de Justicia europeos, en su XXI Conferencia (Praga, 10 y 11 de junio de 1997), que recomendaba al Comité de Ministros apoyar las actividades en relación con la ciberdelincuencia organizadas por el Comité Europeo para Problemas Criminales (CDPC) con el fin de aproximar las legislaciones penales nacionales y permitir la utilización de medios de investigación eficaces en materia de delitos informáticos, así como la Resolución nº 3, adoptada en la XXIII Conferencia de Ministros de Justicia europeos (Londres, 8 y 9 de junio de 2000), que exhortaba a las partes negociadoras a persistir en sus esfuerzos por encontrar soluciones que permitan al mayor número posible de Estados ser partes en el Convenio, y reconocía la necesidad de disponer de un mecanismo rápido y eficaz de cooperación internacional que tenga debidamente en cuenta las exigencias específicas de la lucha contra la ciberdelincuencia;

Teniendo asimismo en cuenta el plan de acción adoptado por los Jefes de Estado y de Gobierno del Consejo de Europa, con ocasión de su segunda Cumbre (Estrasburgo, 10 y 11 de octubre de 1997) con objeto de encontrar respuestas comunes ante el desarrollo de las nuevas tecnologías de la información, basadas en las normas y los valores del Consejo de Europa;

Han convenido en lo siguiente:

Capítulo I – Terminología

Artículo 1 – Definiciones

A los efectos del presente Convenio:

- a. por "sistema informático" se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa;
- b. por "datos informáticos" se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función;
- c. por "proveedor de servicios" se entenderá:
 - i. toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático, y
 - ii. cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo;
- d. por "datos relativos al tráfico" se entenderá todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

Capítulo II – Medidas que deberán adoptarse a nivel nacional

Sección 1 – Derecho penal sustantivo

Título 1 – Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

Artículo 2 – Acceso ilícito

Cada Parte adoptará las medidas legislativas y de otro tipo 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 3 – Interceptación ilícita

Cada Parte adoptará las medidas legislativas y de otro tipo 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 4 – Ataques a la integridad de los datos

1. Cada Parte adoptará las medidas legislativas y de otro tipo 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 5 – Ataques a la integridad del sistema

Cada Parte adoptará las medidas legislativas y de otro tipo 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 6 – Abuso de los dispositivos

1. Cada Parte adoptará las medidas legislativas y de otro tipo 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, difusión u otra forma de puesta a disposición de:
 - i. cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos previstos en los artículos 2 a 5 del presente Convenio;
 - 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 2 a 5; y

- b. la posesión de alguno de los elementos contemplados en los incisos i) o ii) del apartado a) del presente artículo con intención de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2 a 5. 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, difusión o cualquier otra forma de puesta a disposición mencionada en el párrafo 1 del presente artículo no tenga por objeto la comisión de uno de los delitos previstos de conformidad con los artículos 2 a 5 del presente Convenio, 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 cualesquiera otras formas de puesta a disposición de los elementos mencionados en el inciso 1 a) ii) del presente artículo.

Título 2 – delitos informáticos

Artículo 7 – Falsificación informática

Cada Parte adoptará las medidas legislativas y de otro tipo 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 dolosa o delictiva similar para que se considere que existe responsabilidad penal.

Artículo 8 – Fraude informático

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, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.

Título 3 – Delitos relacionados con el contenido

Artículo 9 – Delitos relacionados con la pornografía infantil

1. Cada Parte adoptará las medidas legislativas y de otro tipo 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 difundirla 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 difusión o la transmisión de pornografía infantil a través de un sistema informático;
- d. la adquisición, para uno mismo o para otros, 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.

*Título 4 – Delitos relacionados con infracciones de la propiedad intelectual
y de los derechos afines*

Artículo 10 – Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

1. Cada Parte adoptará las medidas legislativas y de otro tipo 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 OMPI sobre Derecho de Autor, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.
2. Cada Parte adoptará las medidas legislativas y de otro tipo 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 Convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.
3. En circunstancias bien delimitadas, 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.

Título 5 – Otras formas de responsabilidad y de sanción

Artículo 11 – Tentativa y complicidad

1. Cada Parte adoptará las medidas legislativas y de otro tipo 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 aplicación de los artículos 2 a 10 del presente Convenio, con la intención de que dicho delito sea cometido.
2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno toda tentativa deliberada de cometer alguno de los delitos previstos en aplicación de los artículos 3 a 5, 7, 8, 9.1.a) y 9.1.c) del presente Convenio.
3. Las Partes podrán reservarse el derecho a no aplicar, en todo o en parte, el párrafo 2 del presente artículo.

Artículo 12 – Responsabilidad de las personas jurídicas

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que pueda exigirse responsabilidad a las personas jurídicas por los delitos previstos en aplicación del presente Convenio, cuando éstos sean cometidos por cuenta de las mismas por una persona física, ya sea a título individual o como miembro de un órgano de dicha persona jurídica, que ejerza funciones directivas en su seno, en virtud de:
 - a. un poder de representación de la persona jurídica;
 - b. una autorización para tomar decisiones en nombre de la persona jurídica;
 - c. una autorización para ejercer funciones de 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 del presente Convenio 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 13 – Sanciones y medidas

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que los delitos previstos en aplicación de los artículos 2 a 11 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 12.

Sección 2 – Derecho procesal

Título I – Disposiciones comunes

Artículo 14 – Ámbito de aplicación de las disposiciones de procedimiento

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para establecer los poderes y procedimientos previstos en la presente Sección a los efectos de investigación o de procedimientos penales específicos.

2. Salvo que se establezca lo contrario en el artículo 21, cada Parte aplicará los poderes y procedimientos mencionados en el párrafo 1 del presente artículo:

- a. a los delitos previstos en aplicación de los artículos 2 a 11 del presente Convenio;
- b. a cualquier otro delito cometido por medio de un sistema informático; y
- c. a la obtención de pruebas electrónicas de cualquier delito.

3. a. Las Partes podrán reservarse el derecho a aplicar las medidas mencionadas en el artículo 20 únicamente a los delitos o categorías de delitos especificados en su reserva, siempre que el repertorio de dichos delitos o categorías de delitos no sea más reducido que el de los delitos a los que dicha Parte aplique las medidas mencionadas en el artículo 21. Las Partes tratarán de limitar tal reserva de modo que sea posible la más amplia aplicación de la medida mencionada en el artículo 20.

b. Cuando, a causa de las restricciones que imponga su legislación vigente en el momento de la adopción del presente Convenio, una Parte no pueda aplicar las medidas previstas en los artículos 20 y 21 a las comunicaciones transmitidas dentro de un sistema informático de un proveedor de servicios:

- i. que se haya puesto en funcionamiento para un grupo restringido de usuarios, y
- ii. que no emplee las redes públicas de telecomunicación y no esté conectado a otro sistema informático, ya sea público o privado,

dicha Parte podrá reservarse el derecho a no aplicar dichas medidas a esas comunicaciones. Las Partes tratarán de limitar este tipo de reservas de modo que de modo que sea posible la más amplia aplicación de las medidas previstas en los artículos 20 y 21.

Artículo 15 – Condiciones y salvaguardias

1. Cada Parte se asegurará de que la instauración, ejecución y aplicación de los poderes y procedimientos previstos en la presente Sección 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

derivados de las obligaciones que haya asumido cada Parte en virtud del Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) u otros instrumentos internacionales aplicables en materia de derechos humanos, y que deberá integrar el principio de proporcionalidad.

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

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

Título 2 – Conservación rápida de datos informáticos almacenados

Artículo 16 – Conservación rápida de datos informáticos almacenados

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

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

3. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a la persona que custodia los datos o a otra persona encargada de su conservación a mantener en secreto la ejecución de dichos procedimientos durante el tiempo previsto en su derecho interno.

4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Artículo 17 – Conservación y revelación parcial rápidas de los datos relativos al tráfico

1. Con el fin de garantizar la conservación de los datos relativos al tráfico, en aplicación del artículo 16, cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para:

- a. garantizar la conservación rápida de los datos relativos al tráfico, ya sean uno o varios los proveedores de servicios que hayan participado en la transmisión de dicha comunicación; y
- b. asegurar la revelación rápida a la autoridad competente de la Parte, o a una persona designada por dicha autoridad, de un volumen suficiente de datos relativos al tráfico para que dicha Parte pueda identificar tanto a los proveedores de servicios como la vía por la que la comunicación se ha transmitido.

2. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Título 3 – Orden de presentación

Artículo 18 – Orden de presentación

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

- a. a una persona presente en su territorio que comunique determinados datos informáticos que obren en su poder o bajo su control, almacenados en un sistema informático o en un dispositivo de almacenamiento informático; y
- b. a un proveedor que ofrezca sus servicios en el territorio de dicha Parte, que comunique los datos que obren en su poder o bajo su control relativos a los abonados en relación con dichos servicios;

2. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

3. A los efectos del presente artículo, se entenderá por «datos relativos a los abonados» cualquier información, en forma de datos informáticos o de cualquier otro modo, que posea un proveedor de servicios y que se refiera a los abonados de sus servicios, diferentes de los datos relativos al tráfico o al contenido, y que permitan determinar:

- a. el tipo de servicio de comunicación utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio;
- b. la identidad, la dirección postal o situación geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso 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. cualquier otra información relativa al lugar en que se encuentren los equipos de comunicación, disponible en virtud de un contrato o de un acuerdo de prestación de servicio.

Título 4 – Registro y confiscación de datos informáticos almacenados

Artículo 19 – Registro y confiscación de datos informáticos almacenados

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a registrar o a tener acceso de un modo similar:

- a. a todo sistema informático o a parte del mismo, así como a los datos informáticos en él almacenados; y
- b. a todo dispositivo de almacenamiento informático que permita almacenar datos informáticos

en su territorio.

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

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

- a. confiscar u obtener de un modo similar un sistema informático o una parte del mismo, o un dispositivo de almacenamiento informático;
- b. realizar y conservar una copia de esos datos informáticos;
- c. preservar la integridad de los datos informáticos almacenados pertinentes; y
- d. hacer inaccesibles o suprimir dichos datos informáticos del sistema informático consultado.

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

5. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Título 5 – Obtención en tiempo real de datos informáticos

Artículo 20 – Obtención en tiempo real de datos relativos al tráfico

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

- a. a obtener o grabar con medios técnicos existentes en su territorio, y
- b. a obligar a cualquier proveedor de servicios, en la medida de sus capacidades técnicas:
 - i. a obtener o a grabar con medios técnicos existentes en su territorio, o

- ii. a ofrecer a las autoridades competentes su colaboración y su asistencia para obtener o grabar

en tiempo real los datos relativos al tráfico asociados a comunicaciones específicas transmitidas en su territorio por medio de un sistema informático.

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

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

4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Artículo 21 – Interceptación de datos relativos al contenido

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

- a. obtener o grabar con medios técnicos existentes en su territorio, y
- b. obligar a un proveedor de servicios, en la medida de sus capacidades técnicas, a:
 - i. obtener o grabar con 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 los datos relativos al contenido de comunicaciones específicas transmitidas en su territorio por medio de un sistema informático.

2. Cuando una Parte no pueda adoptar las medidas enunciadas en el apartado 1.a) por respeto a los principios establecidos en su ordenamiento jurídico interno, podrá, en su lugar, adoptar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos relativos al contenido de comunicaciones específicas transmitidas en su territorio con medios técnicos existentes en ese territorio.

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

4. Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Sección 3 – Jurisdicción

Artículo 22 – Jurisdicción

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito previsto de conformidad con los artículos 2 a 11 del presente Convenio, cuando el delito se haya cometido:

- a. en su territorio; o
- b. a bordo de un buque que enarbole su pabellón; o
- c. a bordo de una aeronave matriculada según sus leyes; o
- d. por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar en el que se cometió o si ningún Estado tiene competencia territorial respecto del mismo.

2. Las Partes podrán reservarse el derecho a no aplicar, o a aplicar sólo en determinados casos o condiciones, las normas sobre jurisdicción establecidas en los apartados 1.b) a 1.d) del presente artículo o en cualquier parte de dichos apartados.

3. Cada Parte adoptará las medidas que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito mencionado en el párrafo 1 del artículo 24 del presente Convenio cuando el presunto autor del mismo se halle en su territorio y no pueda ser extraditado a otra Parte por razón únicamente de su nacionalidad, previa demanda de extradición.

4. El presente Convenio no excluye ninguna jurisdicción penal ejercida por una Parte de conformidad con su derecho interno.

5. En el caso de que varias Partes reivindiquen su jurisdicción respecto de un presunto delito contemplado en el presente Convenio, las Partes interesadas celebrarán consultas, cuando ello sea oportuno, con el fin de decidir qué jurisdicción es más adecuada para entablar la acción penal.

Capítulo III – Cooperación internacional

Sección 1 – Principios generales

Título 1 – Principios generales relativos a la cooperación internacional

Artículo 23 – Principios generales relativos a la cooperación internacional

Las Partes cooperarán entre sí en la mayor medida posible de conformidad con las disposiciones del presente Capítulo, en aplicación de los instrumentos internacionales pertinentes sobre cooperación internacional en materia penal, de los acuerdos basados en legislación uniforme o recíproca y de su propio derecho interno, a efectos de las investigaciones o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para obtener pruebas en formato electrónico de los delitos.

Título 2 – Principios relativos a la extradición

Artículo 24 – Extradición

1. a. El presente artículo se aplicará a la extradición entre las Partes por los delitos definidos de conformidad con los artículos 2 a 11 del presente Convenio, siempre que sean castigados por la legislación de las dos Partes implicadas con una pena privativa de libertad de una duración de al menos un año, o con una pena más grave.

b. Cuando se aplique una pena mínima diferente en virtud de un tratado de extradición aplicable entre dos o más Partes, incluido el Convenio Europeo de Extradición (STE nº 24), o de un acuerdo basado en legislación uniforme o recíproca, se aplicará la pena mínima prevista en dicho tratado o acuerdo.

2. Se considerará que los delitos descritos en el párrafo 1 del presente artículo están incluidos entre los delitos que pueden dar lugar a extradición en todos los tratados de extradición concluidos entre o por las Partes. Las Partes se comprometerán a incluir dichos delitos entre los que pueden dar lugar a extradición en todos los tratados de extradición que puedan concluir.

3. Cuando una parte que condicione la extradición a la existencia de un tratado reciba una demanda de extradición de otra Parte con la que no ha concluido ningún tratado de extradición, podrá tomar el presente Convenio como fundamento jurídico de la extradición en relación con cualquiera de los delitos previstos en el párrafo 1 del presente artículo.

4. Las Partes que no condicionen la extradición a la existencia de un tratado reconocerán los delitos mencionados en el párrafo 1 del presente artículo como delitos que pueden dar lugar a extradición entre ellas.

5. La extradición estará sujeta a las condiciones previstas en el derecho interno de la Parte requerida o en los tratados de extradición vigentes, incluidos los motivos por los que la Parte requerida puede denegar la extradición.

6. Si se deniega la extradición por un delito mencionado en el párrafo 1 del presente artículo únicamente por razón de la nacionalidad de la persona reclamada o porque la Parte requerida se considera competente respecto de dicho delito, la Parte requerida deberá someter el asunto, a petición de la Parte requirente, a sus autoridades competentes a efectos de la acción penal pertinente, e informará, a su debido tiempo, de la conclusión del asunto a la Parte requirente. Dichas autoridades tomarán su decisión y realizarán sus investigaciones y procedimientos del mismo modo que para cualquier otro delito de naturaleza comparable, de conformidad con la legislación de dicha Parte.

7. a. Cada Parte comunicará al Secretario General del Consejo de Europa, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, el nombre y la dirección de cada autoridad responsable del envío o de la recepción de las demandas de extradición o de detención provisional, en ausencia de tratado.

b. El Secretario General del Consejo de Europa creará y mantendrá actualizado un registro de las autoridades designadas por las Partes. Cada Parte garantizará en todo momento la exactitud de los datos que figuren en el registro.

Título 3 – Principios generales relativos a la asistencia mutua

Artículo 25 – Principios generales relativos a la asistencia mutua

1. Las Partes se prestarán toda la ayuda mutua posible a efectos de las investigaciones o de los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o con el fin de obtener pruebas en formato electrónico de un delito.
2. Cada Parte adoptará asimismo las medidas legislativas y de otro tipo que resulten necesarias para cumplir con las obligaciones establecidas en los artículos 27 a 35.
3. Cada Parte podrá, en caso de urgencia, formular una solicitud de asistencia mutua, o realizar las comunicaciones relativas a la misma a través de medios de comunicación rápidos, como el fax o el correo electrónico, siempre que esos medios ofrezcan niveles suficientes de seguridad y de autenticación (incluido el criptado, en caso necesario), con confirmación oficial posterior si el Estado requerido así lo exige. El Estado requerido aceptará la solicitud y responderá a la misma por cualquiera de esos medios rápidos de comunicación.
4. Salvo en caso de que se disponga expresamente otra cosa en los artículos del presente Capítulo, la asistencia mutua estará sujeta a las condiciones establecidas en el derecho interno de la Parte requerida o en los tratados de asistencia mutua aplicables, incluidos los motivos sobre la base de los cuales la Parte requerida puede rechazar la cooperación. La Parte requerida no deberá ejercer su derecho a rehusar la asistencia mutua en relación con los delitos previstos en los artículos 2 a 11 únicamente porque la solicitud se refiera a un delito que dicha Parte considere de carácter fiscal.
5. Cuando, de conformidad con lo dispuesto en el presente Capítulo, la Parte requerida esté autorizada a condicionar la asistencia mutua a la existencia de doble tipificación penal, se considerará que dicha condición se satisface si el acto que constituye delito, y para el que se solicita la asistencia mutua, está tipificado como tal en su derecho interno, independientemente de que dicho derecho interno incluya o no el delito en la misma categoría o lo denomine o no con la misma terminología que la Parte requirente.

Artículo 26 – Información espontánea

1. Dentro de los límites de su derecho interno y sin que exista demanda previa, una Parte podrá comunicar a otra Parte información obtenida de sus propias investigaciones si considera que ello puede ayudar a la Parte destinataria a iniciar o a concluir investigaciones o procedimientos en relación con delitos previstos de conformidad con el presente Convenio, o cuando dicha información pueda conducir a una petición de cooperación de dicha Parte en virtud del presente Capítulo.
2. Antes de comunicar dicha información, la Parte que la proporciona podrá pedir que sea tratada de forma confidencial o que sólo se utilice bajo ciertas condiciones. Si la Parte destinataria no puede atender a dicha petición, deberá informar de ello a la otra Parte, que decidirá a continuación si, no obstante, debe proporcionar la información. Si la Parte destinataria acepta la información bajo las condiciones establecidas, estará obligada a respetarlas.

Título 4 – Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables

Artículo 27 – Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables

1. En ausencia de tratado de asistencia mutua o de acuerdo basado en legislación uniforme o recíproca en vigor entre la Parte requirente y la Parte requerida, se aplicarán las disposiciones de los párrafos 2 a 9 del presente artículo. Dichas disposiciones no se aplicarán cuando exista un tratado, acuerdo o legislación de este tipo, a menos que las Partes implicadas decidan aplicar en su lugar la totalidad o una parte del resto del presente artículo.
2.
 - a. Cada Parte designará una o varias autoridades centrales encargadas de enviar las solicitudes de asistencia mutua o de responder a las mismas, de ejecutarlas o de remitirlas a las autoridades competentes para su ejecución;
 - b. las autoridades centrales comunicarán directamente entre sí;
 - c. en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, cada Parte comunicará al Secretario General del Consejo de Europa los nombres y direcciones de las autoridades designadas en aplicación del presente párrafo.
 - d. el Secretario General del Consejo de Europa creará y mantendrá actualizado un registro de las autoridades centrales designadas por las Partes. Cada Parte garantizará en todo momento la exactitud de los datos que figuren en el registro.
3. Las solicitudes de asistencia mutua en virtud del presente artículo se ejecutarán de conformidad con el procedimiento especificado por la Parte requirente, salvo cuando dicho procedimiento sea incompatible con la legislación de la Parte requerida.
4. Además de las condiciones o los motivos de denegación previstos en el párrafo 4 del artículo 25, la asistencia mutua puede ser denegada por la Parte requerida:
 - a. si la solicitud tiene que ver con un delito que la Parte requerida considere de carácter político o vinculado a un delito de carácter político; o
 - b. si la Parte requerida estima que acceder a la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.
5. La Parte requerida podrá aplazar su actuación en respuesta a una solicitud si dicha actuación puede perjudicar a investigaciones o procedimientos llevados a cabo por sus autoridades.
6. Antes de denegar o aplazar su cooperación, la Parte requerida estudiará, previa consulta con la Parte requirente cuando proceda, si puede atenderse la solicitud parcialmente o bajo las condiciones que considere necesarias.
7. La Parte requerida informará rápidamente a la Parte requirente del curso que prevé dar a la solicitud de asistencia. Deberá motivar toda denegación o aplazamiento de la misma. La Parte requerida informará asimismo a la Parte requirente de cualquier motivo que imposibilite la ejecución de la asistencia o que pueda retrasarla sustancialmente.

8. La Parte requirente podrá solicitar que la Parte requerida mantenga confidenciales la presentación y el objeto de cualquier solicitud formulada en virtud del presente Capítulo, salvo en la medida en que sea necesario para la ejecución de la misma. Si la Parte requerida no puede acceder a la petición de confidencialidad, deberá informar de ello sin demora a la Parte requirente, quien decidirá a continuación si, no obstante, la solicitud debe ser ejecutada.

9. a. En caso de urgencia, las autoridades judiciales de la Parte requirente podrán dirigir directamente a las autoridades homólogas de la Parte requerida las solicitudes de asistencia y las comunicaciones relativas a las mismas. En tales casos, se remitirá simultáneamente una copia a la autoridad central de la Parte requerida a través de la autoridad central de la Parte requirente.

b. Toda solicitud o comunicación en virtud del presente párrafo podrá formularse a través de la Organización Internacional de Policía Criminal (Interpol).

c. Cuando se formule una solicitud en aplicación del apartado a) del presente artículo y la autoridad no tenga competencia para tratarla, la remitirá a la autoridad nacional competente e informará directamente de ello a la Parte requirente.

d. Las solicitudes o comunicaciones realizadas en aplicación del presente párrafo que no impliquen medidas coercitivas podrán ser transmitidas directamente por las autoridades competentes de la Parte requirente a las autoridades competentes de la Parte requerida.

e. En el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, las Partes podrán informar al Secretario General del Consejo de Europa de que, en aras de la eficacia, las solicitudes formuladas en virtud del presente párrafo deberán dirigirse a su autoridad central.

Artículo 28 – Confidencialidad y restricciones de uso

1. En ausencia de tratado de asistencia mutua o de acuerdo basado en legislación uniforme o recíproca en vigor entre la Parte requirente y la Parte requerida, se aplicarán las disposiciones del presente artículo. Dichas disposiciones no se aplicarán cuando exista un tratado, acuerdo o legislación de este tipo, a menos que las Partes interesadas decidan aplicar en su lugar la totalidad o una parte del presente artículo.

2. La Parte requerida podrá supeditar la transmisión de información o de material en respuesta a una solicitud al cumplimiento de las siguientes condiciones:

- a. que se preserve su confidencialidad cuando la solicitud de asistencia no pueda ser atendida en ausencia de dicha condición; o
- b. que no se utilicen para investigaciones o procedimientos distintos a los indicados en la solicitud.

3. Si la Parte requirente no pudiera satisfacer alguna de las condiciones mencionadas en el párrafo 2, informará de ello sin demora a la Parte requerida, quien determinará a continuación si, no obstante, la información ha de ser proporcionada. Si la Parte requirente acepta esta condición, estará obligada a cumplirla.

4. Toda Parte que proporcione información o material supeditado a alguna de las condiciones mencionadas en el párrafo 2 podrá exigir a la otra Parte precisiones sobre el uso que haya hecho de dicha información o material en relación con dicha condición.

Sección 2 – Disposiciones específicas

Título 1 – Asistencia mutua en materia de medidas provisionales

Artículo 29 – Conservación rápida de datos informáticos almacenados

1. Una Parte podrá solicitar a otra Parte que ordene o imponga de otro modo la conservación rápida de datos almacenados por medio de sistemas informáticos que se encuentren en el territorio de esa otra Parte, y en relación con los cuales la Parte requiriente tenga intención de presentar una solicitud de asistencia mutua con vistas al registro o al acceso por un medio similar, la confiscación o la obtención por un medio similar, o a la revelación de dichos datos.

2. En toda solicitud de conservación formulada en virtud del párrafo 1 deberá precisarse:

- a. la autoridad que solicita la conservación;
- b. el delito objeto de la investigación o de procedimientos penales y una breve exposición de los hechos relacionados con el mismo;
- c. los datos informáticos almacenados que deben conservarse y su relación con el delito;
- d. toda información disponible que permita identificar al responsable de la custodia de los datos informáticos almacenados o el emplazamiento del sistema informático;
- e. la necesidad de la medida de conservación; y
- f. que la Parte tiene intención de presentar una solicitud de asistencia mutua con vistas al registro o al acceso por un medio similar, a la confiscación o a la obtención por un medio similar, o a la revelación de los datos informáticos almacenados.

3. Tras recibir la solicitud de otra Parte, la Parte requerida deberá adoptar todas las medidas adecuadas para proceder sin demora a la conservación de los datos solicitados, de conformidad con su derecho interno. A los efectos de responder a solicitudes de este tipo no se requiere la doble tipificación penal como condición para proceder a la conservación.

4. Cuando una Parte exige la doble tipificación penal como condición para atender a una solicitud de asistencia mutua con vistas al registro o al acceso por un medio similar, a la confiscación o a la obtención por un medio similar o a la revelación de los datos almacenados en relación con delitos diferentes de los previstos de conformidad con los artículos 2 a 11 del presente Convenio, podrá reservarse el derecho a denegar la solicitud de conservación en virtud del presente artículo en caso de que tenga motivos para creer que, en el momento de la revelación de los datos, no se cumplirá la condición de la doble tipificación penal.

5. Asimismo, las solicitudes de conservación sólo podrán ser denegadas si:

- a. la solicitud se refiere a un delito que la Parte requerida considera de carácter político o vinculado a un delito de carácter político; o

- b. la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.

6. Cuando la Parte requerida considere que la conservación por sí sola de los datos no bastará para garantizar su disponibilidad futura, o que pondrá en peligro la confidencialidad de la investigación de la Parte requirente, o causará cualquier otro perjuicio a la misma, informará de ello rápidamente a la Parte requirente, quien determinará a continuación la conveniencia, no obstante, de dar curso a la solicitud.

7. Las medidas de conservación adoptadas en respuesta a solicitudes como la prevista en el párrafo 1 serán válidas por un periodo mínimo de 60 días, con el fin de que la Parte requirente pueda presentar una solicitud con vistas al registro o el acceso por un medio similar, la confiscación o la obtención por un medio similar, o la revelación de los datos. Una vez recibida la solicitud, los datos deberán conservarse hasta que se tome una decisión sobre la misma.

Artículo 30 – Revelación rápida de datos conservados

1. Si, al ejecutar una solicitud formulada de conformidad con el artículo 29 para la conservación de datos relativos al tráfico de una determinada comunicación la Parte requerida descubriera que un proveedor de servicios de otro Estado ha participado en la transmisión de dicha comunicación, dicha Parte revelará rápidamente a la Parte requirente un volumen suficiente de datos relativos al tráfico para que pueda identificarse al proveedor de servicios, así como la vía por la que la comunicación ha sido transmitida.

2. La revelación de datos relativos al tráfico en aplicación del párrafo 1 sólo podrá ser denegada si:

- a. la solicitud se refiere a un delito que la Parte requerida considera de carácter político o vinculado a un delito de carácter político; o
- b. la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.

Título 2 – Asistencia mutua en relación con los poderes de investigación

Artículo 31 – Asistencia mutua en relación con el acceso a datos almacenados

1. Una Parte podrá solicitar a otra Parte el registro o el acceso de un modo similar, la confiscación o la obtención de un modo similar o la revelación de datos almacenados por medio de un sistema informático que se encuentre en el territorio de esa otra Parte, incluidos los datos conservados de conformidad con el artículo 29.

2. La Parte requerida responderá a la solicitud aplicando los instrumentos internacionales, acuerdos y legislación mencionados en el artículo 23, así como de conformidad con las disposiciones pertinentes del presente Capítulo.

3. La solicitud deberá responderse lo más rápidamente posible en los siguientes casos:

- a. cuando existan motivos para creer que los datos pertinentes están particularmente expuestos al riesgo de pérdida o de modificación; o

- b. cuando los instrumentos, acuerdos o legislación mencionados en el párrafo 2 prevean una cooperación rápida.

Artículo 32 – Acceso transfronterizo a datos almacenados, con consentimiento o cuando sean accesibles al público

Una Parte podrá, sin autorización de otra:

- a. tener acceso a datos informáticos almacenados accesibles al público (fuente abierta), independientemente de la ubicación geográfica de los mismos; o
- b. tener acceso a datos informáticos almacenados en otro Estado, o recibirlos, a través de un sistema informático situado en su territorio, si dicha Parte obtiene el consentimiento lícito y voluntario de la persona legalmente autorizada a revelárselos por medio de ese sistema informático.

Artículo 33 – Asistencia mutua para la obtención en tiempo real de datos relativos al tráfico

1. Las Partes se prestarán asistencia mutua para la obtención en tiempo real de datos relativos al tráfico asociados a comunicaciones específicas transmitidas en su territorio por medio de un sistema informático. A reserva de las disposiciones del párrafo 2, dicha asistencia mutua estará sujeta a las condiciones y procedimientos previstos en el derecho interno.

2. Cada Parte prestará dicha asistencia al menos en relación con los delitos para los cuales sería posible la obtención en tiempo real de datos relativos al tráfico en situaciones análogas a nivel interno.

Artículo 34 – Asistencia mutua en relación con la interceptación de datos relativos al contenido

Las Partes se prestarán asistencia mutua, en la medida en que lo permitan sus tratados y leyes internas aplicables, para la obtención o el registro en tiempo real de datos relativos al contenido de comunicaciones específicas transmitidas por medio de un sistema informático.

Título 3 – Red 24/7

Artículo 35 – Red 24/7

1. Cada Parte designará un punto de contacto localizable las 24 horas del día, siete días a la semana, con el fin de garantizar una asistencia inmediata para investigaciones relativas a delitos vinculados a sistemas y datos informáticos, o para obtener las pruebas en formato electrónico de un delito. Esta asistencia comprenderá toda acción que facilite las medidas que figuran a continuación, o su aplicación directa si lo permite el derecho y la práctica internos:

- a. asesoramiento técnico;
- b. conservación de datos, de conformidad con los artículos 29 y 30; y
- c. obtención de pruebas, suministro de información de carácter jurídico y localización de sospechosos.

2. a. El punto de contacto de una Parte dispondrá de los medios para comunicarse con el punto de contacto de otra Parte siguiendo un procedimiento acelerado.

b. Si el punto de contacto designado por una Parte no depende de la autoridad o autoridades de dicha Parte responsables de la asistencia mutua internacional o de la extradición, dicho punto de contacto se asegurará de poder actuar coordinadamente con esta o estas autoridades por medio de un procedimiento acelerado.

3. Cada Parte garantizará la disponibilidad de personal formado y equipado con objeto de facilitar el funcionamiento de la red.

Capítulo IV – Cláusulas finales

Artículo 36 – Firma y entrada en vigor

1. El presente Convenio está abierto a la firma de los Estados miembros del Consejo de Europa y de los Estados no miembros que hayan participado en su elaboración.

2. El presente Convenio estará sujeto a ratificación, aceptación o aprobación. Los instrumentos de ratificación, aceptación o aprobación se depositarán en poder del Secretario General del Consejo de Europa.

3. El presente Convenio entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que cinco Estados, de los cuales al menos tres deberán ser miembros del Consejo de Europa, hayan expresado su consentimiento para quedar vinculados por el Convenio, de conformidad con lo dispuesto en los párrafos 1 y 2.

4. Para todo Estado signatario que exprese ulteriormente su consentimiento para quedar vinculado por el Convenio, éste entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que haya expresado dicho consentimiento, de conformidad con lo dispuesto en los párrafos 1 y 2.

Artículo 37 – Adhesión al Convenio

1. A partir de la entrada en vigor del presente Convenio, el Comité de Ministros del Consejo de Europa podrá, previa consulta con los Estados contratantes del Convenio y habiendo obtenido su consentimiento unánime, invitar a adherirse al presente Convenio a cualquier Estado que no sea miembro del Consejo de Europa y que no haya participado en su elaboración. La decisión se adoptará respetando la mayoría establecida en el artículo 20.d del Estatuto del Consejo de Europa y con el voto unánime de los representantes de los Estados contratantes con derecho a formar parte del Comité de Ministros.

2. Para todo Estado que se adhiera al Convenio de conformidad con el párrafo 1 precedente, el Convenio entrará en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha del depósito del instrumento de adhesión en poder del Secretario General del Consejo de Europa.

Artículo 38 – Aplicación territorial

1. En el momento de la firma o del depósito del instrumento de ratificación, aceptación, aprobación o adhesión, todo Estado podrá designar el territorio o los territorios a los que se aplicará el presente Convenio.
2. Posteriormente, todo Estado podrá, en cualquier momento y por medio de una declaración dirigida al Secretario General del Consejo de Europa, hacer extensiva la aplicación del presente Convenio a cualquier otro territorio especificado en la declaración. El Convenio entrará en vigor respecto de dicho territorio el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido la declaración.
3. Toda declaración formulada en virtud de los dos párrafos precedentes podrá ser retirada, respecto de cualquier territorio especificado en la misma, mediante notificación dirigida al Secretario General del Consejo de Europa. La retirada surtirá efecto el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido la notificación.

Artículo 39 – Efectos del Convenio

1. El objeto del presente Convenio es completar los tratados o acuerdos multilaterales o bilaterales aplicables entre las Partes, incluidas las disposiciones:
 - del Convenio Europeo de Extradición, abierto a la firma el 13 de diciembre de 1957 en París (STE n° 24)
 - del Convenio Europeo de Asistencia Judicial en Materia Penal, abierto a la firma el 20 de abril de 1959 en Estrasburgo (STE n° 30),
 - del Protocolo adicional al Convenio Europeo de Asistencia Judicial en Materia Penal, abierto a la firma el 17 de marzo de 1978 en Estrasburgo (STE n° 99).
2. Si dos o más Partes han celebrado ya un acuerdo o un tratado relativo a las cuestiones contempladas en el presente Convenio, o han regulado de otro modo sus relaciones al respecto, o si lo hacen en el futuro, podrán asimismo aplicar el citado acuerdo o tratado, o regular sus relaciones de conformidad con el mismo, en lugar del presente Convenio. No obstante, cuando las Partes regulen sus relaciones respecto de las cuestiones objeto del presente Convenio de forma distinta a la prevista en el mismo, lo harán de modo que no sea incompatible con los objetivos y principios del Convenio.
3. Nada de lo dispuesto en el presente Convenio afectará a otros derechos, restricciones, obligaciones y responsabilidades de cada Parte.

Artículo 40 – Declaraciones

Mediante declaración por escrito dirigida al Secretario General del Consejo de Europa, cualquier Estado podrá declarar, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, que se acoge a la facultad de exigir, llegado el caso, uno o varios elementos complementarios previstos en los artículos 2, 3, 6.1.b), 7, 9.3 y 27.9.e).

Artículo 41 – Cláusula federal

1. Un Estado federal podrá reservarse el derecho a cumplir las obligaciones especificadas en el Capítulo II del presente Convenio en la medida en que éstas sean compatibles con los principios fundamentales por los que se rijan las relaciones entre su gobierno central y los estados que lo constituyen u otras entidades territoriales análogas, a condición de que pueda garantizar la cooperación según lo previsto en el Capítulo III.

2. Cuando formule una reserva en virtud del párrafo 1, un Estado federal no podrá hacer uso de los términos de dicha reserva para excluir o reducir de manera sustancial sus obligaciones en virtud del Capítulo II. En todo caso, se dotará de medios amplios y efectivos para aplicar las medidas previstas en el citado Capítulo.

3. En lo relativo a las disposiciones del presente Convenio cuya aplicación sea competencia legislativa de cada uno de los estados constituyentes u otras entidades territoriales análogas, que no estén obligados por el sistema constitucional de la federación a adoptar medidas legislativas, el gobierno federal pondrá dichas disposiciones en conocimiento de las autoridades competentes de los estados constituyentes junto con su opinión favorable, alentándolas a adoptar las medidas adecuadas para su aplicación.

Artículo 42 – Reservas

Mediante notificación por escrito dirigida al Secretario del Consejo de Europa, cualquier Estado podrá declarar, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, que se acoge a una o varias de las reservas previstas en el párrafo 2 del artículo 4, el párrafo 3 del artículo 6, el párrafo 4 del artículo 9, el párrafo 3 del artículo 10, el párrafo 3 del artículo 11, el párrafo 3 del artículo 14, el párrafo 2 del artículo 22, el párrafo 4 del artículo 29 y el párrafo 1 del artículo 41. No podrá formularse ninguna otra reserva.

Artículo 43 – Mantenimiento y retirada de las reservas

1. Una Parte que haya formulado una reserva de conformidad con el artículo 42 podrá retirarla total o parcialmente mediante notificación por escrito dirigida al Secretario General del Consejo de Europa. Dicha retirada surtirá efecto en la fecha en que el Secretario General reciba la notificación. Si en la notificación se indica una fecha a partir de la cual ha de hacerse efectiva la retirada de una reserva y esta fecha es posterior a la fecha en la que el Secretario General ha recibido la notificación, la retirada se hará efectiva en dicha fecha posterior.

2. Una Parte que haya formulado una reserva de las mencionadas en el artículo 42 retirará dicha reserva, total o parcialmente, tan pronto como lo permitan las circunstancias.

3. El Secretario General del Consejo de Europa podrá solicitar periódicamente a las Partes que hayan formulado una o varias reservas conforme a lo dispuesto en el artículo 42, información sobre las perspectivas de su retirada.

Artículo 44 – Enmiendas

1. Cada Parte podrá proponer enmiendas al presente Convenio, que el Secretario General del Consejo de Europa comunicará a los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del presente Convenio y a cualquier Estado que se haya adherido o que haya sido invitado a adherirse de conformidad con lo dispuesto en el artículo 37.

2. Toda enmienda propuesta por cualquiera de las Partes será comunicada al Comité Europeo para Problemas Criminales (CDPC), quien someterá al Comité de Ministros su opinión sobre la enmienda propuesta.

3. El Comité de Ministros examinará la enmienda propuesta y la opinión presentada por el CDPC y, previa consulta con los Estados no miembros Partes en el presente Convenio, podrá adoptar la enmienda.

4. El texto de cualquier enmienda adoptada por el Comité de Ministros de conformidad con lo dispuesto en el párrafo 3 del presente artículo será remitido a las Partes para su aceptación.

5. Toda enmienda adoptada de conformidad con el párrafo 3 del presente artículo entrará en vigor treinta días después de que todas las Partes hayan informado al Secretario General de su aceptación.

Artículo 45 – Solución de controversias

1. Se mantendrá informado al Comité Europeo para Problemas Criminales (CDPC) del Consejo de Europa acerca de la interpretación y la aplicación del presente Convenio.

2. En caso de controversia entre las Partes sobre la interpretación o la aplicación del presente Convenio, las Partes intentarán llegar a un acuerdo mediante negociación o por cualquier otro medio pacífico de su elección, incluida la sumisión de la controversia al CDPC, a un tribunal arbitral cuyas decisiones serán vinculantes para las Partes en litigio, o a la Corte Internacional de Justicia, según acuerden dichas Partes.

Artículo 46 – Consultas entre las Partes

1. Las Partes se consultarán periódicamente, según sea necesario, con el fin de facilitar:

- a. la utilización y la aplicación efectivas del presente Convenio, incluida la identificación de cualquier problema al respecto, así como las repercusiones de toda declaración o reserva formulada de conformidad con el presente Convenio;
- b. el intercambio de información sobre novedades jurídicas, políticas o técnicas importantes observadas en el ámbito de la delincuencia informática y la obtención de pruebas en formato electrónico;
- c. el estudio de la posibilidad de ampliar o enmendar el Convenio.

2. Se informará periódicamente al Comité Europeo para Problemas Criminales (CDPC) del resultado de las consultas mencionadas en el párrafo 1.

3. En caso necesario, el Comité Europeo para Problemas Criminales (CDPC) facilitará las consultas mencionadas en el párrafo 1 y adoptará las medidas necesarias para ayudar a las Partes en sus esfuerzos por ampliar o enmendar el Convenio. Expirado un

plazo de tres años como máximo desde la entrada en vigor del presente Convenio, el CDPC procederá, en cooperación con las Partes, a una revisión de todas las disposiciones de la Convención y propondrá, si procede, las enmiendas pertinentes.

4. Salvo cuando el Consejo de Europa los asuma, los gastos que ocasione la aplicación de las disposiciones del párrafo 1 serán sufragados por las Partes, en la forma que ellas mismas determinen.

5. Las Partes recibirán asistencia del Secretario del Consejo de Europa en el ejercicio de las funciones que dimanen del presente artículo.

Artículo 47 – Denuncia

1. Las Partes podrán denunciar en cualquier momento el presente Convenio mediante notificación dirigida al Secretario General del Consejo de Europa.

2. Dicha denuncia surtirá efecto el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido la notificación.

Artículo 48 – Notificación

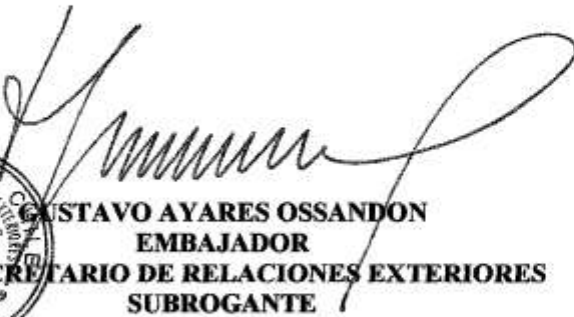

El Secretario General del Consejo de Europa notificará a los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del presente Convenio, así como a cualquier Estado que se haya adherido o que haya sido invitado a adherirse al mismo:

- a. cualquier firma;
- b. el depósito de cualquier instrumento de ratificación, aceptación, aprobación o adhesión;
- c. cualquier fecha de entrada en vigor del presente Convenio de conformidad con los artículos 36 y 37;
- d. cualquier declaración presentada de conformidad con el artículo 40 o cualquier reserva formulada en virtud del artículo 42;
- e. cualquier otro acto, notificación o comunicación relativos al presente Convenio.

En fe de lo cual, los infrascritos, debidamente autorizados a tal efecto, firman el presente Convenio.

Hecho en Budapest, el 23 de noviembre de 2001, en versión francesa e inglesa, ambos textos igualmente auténticos, y en un ejemplar único que se depositará en los archivos del Consejo de Europa. El Secretario General del Consejo de Europa remitirá copia certificada a cada uno de los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del Convenio y a cualquier Estado invitado a adherirse al mismo.

CONFORME CON SU ORIGINAL


 **GUSTAVO AYARES OSSANDON**
EMBAJADOR
SUBSECRETARIO DE RELACIONES EXTERIORES
SUBROGANTE

SANTIAGO, 18 de noviembre de 2015.