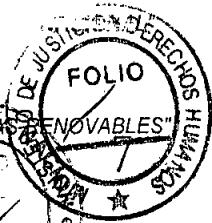
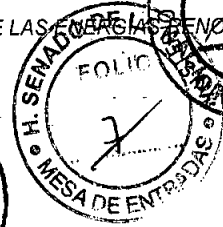


El Poder Ejecutivo
Nacional

"2017 - AÑO DE LAS ENERGÍAS RENOVABLES"



ANEXO I

CONVENIO SOBRE CIBERDELITO

- 27411

M. J. y D. H.

[Handwritten signature]



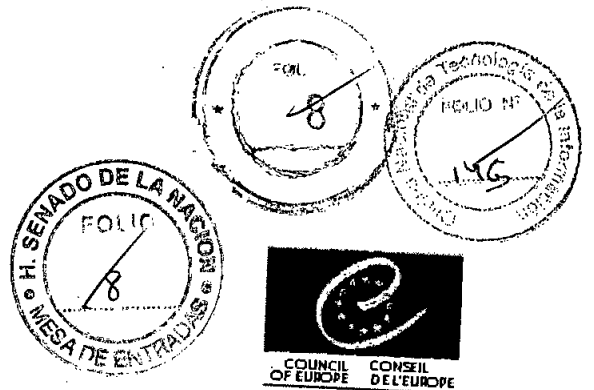
[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

Johnston
James



27411

TRADUCCIÓN PÚBLICA

Convenio sobre ciberdelito

Budapest, 23.XI.2001

Preámbulo

Los Estados miembros del Consejo de Europa y los otros Estados firmantes,

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 parte en este Convenio;

Convencidos de la necesidad de llevar a cabo, con prioridad, una política penal común destinada a prevenir el delito en el ciberespacio y, en particular, de hacerlo mediante la adopción de una legislación apropiada y la mejora de la cooperación internacional;

Conscientes de los profundos cambios suscitados por el incremento, la convergencia y la mundialización permanente de las redes informáticas;

Preocupados por el riesgo de que las redes informáticas y la información electrónica sean utilizadas igualmente para cometer infracciones penales y que las pruebas de dichas infracciones sean almacenadas y transmitidas por medio de esas redes;

Reconociendo la necesidad de una cooperación entre los Estados y la industria privada en la lucha contra el ciberdelito y la necesidad de proteger los intereses legítimos vinculados al desarrollo de las tecnologías de la información;

Estimando que una lucha bien organizada contra el ciberdelito requiere una cooperación internacional en materia penal acrecentada, rápida y eficaz;

Convencidos de que el presente Convenio es necesario para prevenir los actos atentatorios de la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, de las redes y de los datos, así como el uso fraudulento de tales sistemas, redes y datos, asegurando la incriminación de dichos



ES COPIA FIEL

ICH
ICA

PLAZ
P 00

MA
INSGT

comportamientos, como los descritos en el presente Convenio, y la atribución de poderes suficientes para permitir una lucha eficaz contra estas infracciones penales, facilitando la detección, la investigación y la persecución, tanto a nivel nacional como internacional, y previendo algunas disposiciones materiales al objeto de una cooperación internacional rápida y fiable;

Persuadidos de la necesidad de garantizar un equilibrio adecuado entre los intereses de la acción represiva y el respeto de los derechos fundamentales del hombre, como los garantizados en el Convenio para la protección de los derechos del hombre y de las libertades fundamentales del Consejo de Europa (1950), en el Pacto internacional relativo a los derechos civiles y políticos de las Naciones Unidas (1966), así como en otros convenios internacionales aplicables en materia de derechos del hombre, que reafirman el derecho de no ser perseguido por la opinión, el derecho a la libertad de expresión, incluida la libertad de buscar, obtener y comunicar informaciones e ideas de toda naturaleza, sin consideración de fronteras, así como el derecho al respeto de la vida privada;

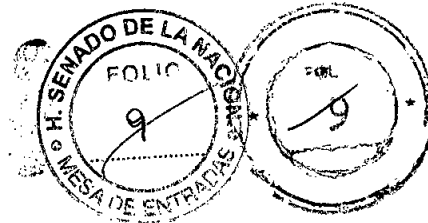
Conscientes, igualmente, de la protección de los datos personales, como la que confiere, por ejemplo, el Convenio de 1981 del Consejo de Europa para la protección de las personas en lo referente al tratamiento automatizado de los datos de carácter personal;

Considerando el Convenio de Naciones Unidas relativo a los derechos del niño y el Convenio de la Organización Internacional del Trabajo sobre la prohibición de las peores formas de trabajo infantil (1999);

Teniendo en cuenta los convenios existentes del Consejo de Europa sobre la cooperación en materia penal, así como otros tratados similares suscritos entre los Estados miembros del Consejo de Europa y otros Estados, y subrayando que el presente Convenio tiene por objeto completarlos con el fin de hacer más eficaces las investigaciones y procedimientos penales relativos a las infracciones penales vinculadas a sistemas y datos informáticos, así como permitir la recogida de pruebas electrónicas de una infracción penal;

Adoptando las recientes iniciativas destinadas a mejorar la comprensión y la cooperación internacional para la lucha contra el cibercrimen y, en particular, las acciones organizadas por las Naciones Unidas, la OCDE, la Unión europea y el G8;

Recordando la Recomendación N.º (85) 10 sobre la aplicación práctica del Convenio europeo de ayuda mutua judicial en materia penal respecto a las comisiones rogatorias para la vigilancia de las telecomunicaciones, la Recomendación N.º (88) 2 sobre medidas dirigidas a combatir la piratería en el ámbito de los derechos de autor y de los derechos afines, la Recomendación N.º (87) 15 dirigida a regular la utilización de datos de carácter personal en el sector de la policía, la Recomendación N.º (95) 4 sobre la protección de los datos de carácter personal en el sector de los servicios de telecomunicación, teniendo en cuenta, en particular, los servicios telefónicos y la Recomendación N.º (89) 9 sobre la delincuencia relacionado con las computadoras, que indica a los legisladores nacionales los principios rectores para definir ciertos delitos



informáticos, así como la Recomendación N.º (95) 13 relativa a los problemas de procedimiento penal vinculados a las tecnologías de la información;

Vista la Resolución N.º 1, adoptada por los Ministros europeos de Justicia, en su 21ª Conferencia (Praga, junio 1997), que recomienda al Comité de Ministros mantener las actividades organizadas por el Comité europeo para los problemas penales (CDPC) relativas al cibercrimen a fin de acercar las legislaciones penales nacionales y permitir la utilización de medios de investigación eficaces en materia de infracciones informáticas, así como la Resolución N.º 3, adoptada en la 23ª Conferencia de Ministros europeos de Justicia (Londres, junio 2000), que alienta a las partes negociadoras a persistir en sus esfuerzos al objeto de encontrar soluciones adecuadas, que permitan al mayor número posible de Estados ser partes en el Convenio y reconoce la necesidad de disponer de un mecanismo rápido y eficaz de cooperación internacional, que tenga en cuenta las específicas exigencias de la lucha contra el cibercrimen;

Tomando igualmente en cuenta el Plan de acción adoptado por los Jefes de Estado y de gobierno del Consejo de Europa, con ocasión de su Décima Cumbre (Estrasburgo, 10-11 octubre 1997) a fin de buscar respuestas comunes al desarrollo de las nuevas tecnologías de la información, fundadas sobre las normas y los valores del Consejo de Europa;

Han convenido lo siguiente:

Capítulo I – Terminología

Artículo 1 – Definiciones

A los efectos del presente Convenio, la expresión:

- a. "sistema informático" designa todo dispositivo aislado o conjunto de dispositivos interconectados o unidos, que aseguran, en ejecución de un programa, el tratamiento automatizado de datos;
- b. "datos informáticos" designa toda representación de hechos, informaciones o conceptos expresados bajo una forma que se preste a tratamiento informático, incluido un programa destinado a hacer que un sistema informático ejecute una función;
- c. "prestador de servicio" ⁽¹⁾ designa:
 - i. toda entidad pública o privada que ofrece a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático;
 - ii. cualquier otra entidad que trate o almacene datos informáticos para ese servicio de comunicación o sus usuarios;



[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

ES COPIA FIEL

d. "datos de tráfico" ⁽²⁾ designa todos los datos que tienen relación con una comunicación por medio de un sistema informático, producidos por este último, en cuanto elemento de la cadena de comunicación, indicando el origen, el destino, el itinerario, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

Capítulo II – Medidas que deben ser adoptadas a nivel nacional

Sección 1 – Derecho penal material

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

Artículo 2 – Acceso ilícito

Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, el acceso doloso ⁽³⁾ y sin autorización a todo o parte de un sistema informático. Las Partes podrán exigir que la infracción sea cometida con vulneración de medidas de seguridad, con la intención de obtener los datos informáticos o con otra intención delictiva, o también podrán requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático.

Artículo 3 – Interceptación ilícita

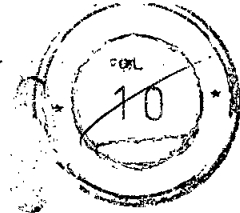
Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la interceptación, dolosa y sin autorización, cometida a través de medios técnicos, de datos informáticos – en transmisiones no públicas– en el destino, origen o en el interior de un sistema informático, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporta tales datos informáticos. Las Partes podrán exigir que la infracción sea cometida con alguna intención delictiva o también podrán requerir que la infracción se perpetre en un sistema informático conectado a otro sistema informático.

Artículo 4 – Atentados contra la integridad de los datos

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la conducta de dañar, borrar, deteriorar, alterar o suprimir dolosamente y sin autorización los datos informáticos.

2. Las Partes podrán reservarse el derecho a exigir que el comportamiento descrito en el párrafo primero ocasione daños que puedan calificarse de graves.

Artículo 5 – Atentados contra la integridad del sistema



Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la obstaculización grave, cometida de forma dolosa sin autorización, del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos.



Artículo 6 - Abuso de equipos e instrumentos técnicos (4)

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, las siguientes conductas cuando éstas sean cometidas dolosamente y sin autorización:

a. la producción, venta, obtención para su utilización, importación, difusión u otras formas de puesta a disposición:

i. de un dispositivo, incluido un programa informático, principalmente concebido o adaptado para permitir la comisión de una de las infracciones establecidas en los artículos 2 a 5 arriba citados;

ii. de una palabra de paso (contraseña), de un código de acceso o de datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con la intención de utilizarlos como medio para cometer alguna de las infracciones previstas en los artículos 2 a 5; y

b. la posesión de alguno de los elementos descritos en los párrafos (a) (1) o (2) con la intención de utilizarlos como medio para cometer alguna de las infracciones previstas en los artículos 2-5. Los Estados podrán exigir en su derecho interno que concurra un determinado número de elementos para que de origen a una responsabilidad penal (5).

2. Lo dispuesto en el presente artículo no generará responsabilidad penal cuando la producción, venta, obtención para la utilización, importación, difusión u otras formas de puesta a disposición mencionadas en el párrafo 1 no persigan la comisión de una infracción prevista en los artículos 2 a 5 del presente Convenio, como en el caso de ensayos o de la protección de un sistema informático.

3. Las Partes podrán reservarse el derecho de no aplicar el párrafo 1, a condición de que dicha reserva no recaiga sobre la venta, distribución o cualesquiera otras formas de puesta a disposición de los elementos mencionados en el párrafo 1 (a)(2).

Título 2 - Infracciones informáticas

Artículo 7 - Falsedad informática



[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

ES COPIA FIEL

[Handwritten signature]

Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la introducción, alteración, borrado o supresión dolosa y sin autorización de datos informáticos, generando datos no auténticos, con la intención de que sean percibidos o utilizados a efectos legales como auténticos, con independencia de que sean directamente legibles e inteligibles. Las Partes podrán reservarse el derecho a exigir la concurrencia de un ánimo fraudulento o de cualquier otro ánimo similar para que de origen a una responsabilidad penal.

Artículo 8 – Estafa informática

Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la producción de un perjuicio patrimonial a otro, de forma dolosa y sin autorización, a través de:

a. la introducción, alteración, borrado o supresión de datos informáticos,

b. cualquier forma de atentado al funcionamiento de un sistema informático,

con la intención, fraudulenta o delictiva, de obtener sin autorización un beneficio económico para sí mismo o para un tercero.

Título 3 – Infracciones relativas al contenido

Artículo 9 – Infracciones relativas a la pornografía infantil

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, las siguientes conductas cuando éstas sean cometidas dolosamente y sin autorización:

a. la producción de pornografía infantil con la intención de difundirla a través de un sistema informático;

b. el ofrecimiento 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. el hecho de procurarse o de procurar a otro pornografía infantil a través de un sistema informático;

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



2. A los efectos del párrafo 1 arriba descrito, la «pornografía infantil» comprende cualquier material pornográfico que represente de manera visual:

- a. un menor adoptando un comportamiento sexualmente explícito;
- b. una persona que aparece como un menor adoptando un comportamiento sexualmente explícito ⁽⁶⁾;
- c. unas imágenes realistas que representen un menor adoptando un comportamiento sexualmente explícito ⁽⁷⁾.



3. A los efectos del párrafo 2 arriba descrito, el término «menor» designa cualquier persona menor de 18 años. Las Partes podrán exigir un límite de edad inferior, que debe ser como mínimo de 16 años.

4. Los Estados podrán reservarse el derecho de no aplicar, en todo o en parte, los párrafos 1 (d) y 1 (e) y 2 (b) y 2 (c).

Título 4 - Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines

Artículo 10 - Infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos afines

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, los atentados a la propiedad intelectual definida por la legislación de cada Estado, conforme a las obligaciones que haya asumido por aplicación de la Convención Universal sobre los Derechos de Autor, revisada en París el 24 de julio de 1971, del 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 OMPI sobre Derecho de Autor, a excepción de cualquier derecho moral conferido por dichas Convenciones, cuando tales actos sean cometidos deliberadamente, a escala comercial y a través de un sistema informático.

2. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, los atentados a los derechos afines definidos por la legislación de cada Estado, conforme 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, hecha en Roma (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 dichas Convenciones, cuando tales actos sean cometidos deliberadamente, a escala comercial y a través de un sistema informático.



[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

ES COPIA FIEL

3. Las Partes podrán, de concurrir determinadas circunstancias, reservarse el derecho de no imponer responsabilidad penal en aplicación de los párrafos 1 y 2 del presente artículo, siempre que se disponga de otros recursos eficaces para su represión y que dicha reserva no comporte infracción de las obligaciones internacionales que incumban al Estado por aplicación de los instrumentos internacionales mencionados en los párrafos 1 y 2 del presente artículo.

Título 5 – Otras formas de responsabilidad y sanción

Artículo 11 – Tentativa y complicidad

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, cualquier acto de complicidad que sea cometido dolosamente y con la intención de favorecer la perpetración de alguna de las infracciones establecidas en los artículos 2 a 10 del presente Convenio.

2. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para prever como infracción penal, conforme a su derecho interno, la tentativa dolosa de cometer una de las infracciones establecidas en los artículos 3 a 5, 7, 8, 9 (1) a y 9 (1) c del presente Convenio.

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

Artículo 12 – Responsabilidad de las personas jurídicas

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para permitir que las personas jurídicas puedan ser tenidas por responsables de las infracciones establecidas en el presente Convenio, cuando éstas sean cometidas por una persona física, actuando ya sea a título individual, ya sea como miembro de un órgano de la persona jurídica, que ejerce un poder de dirección en su seno, cuyo origen se encuentre en:

- 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 control en el seno de la persona jurídica.

2. Fuera de los casos previstos en el párrafo 1, las Partes adoptarán las medidas necesarias para asegurar que una persona jurídica puede ser tenida por responsable cuando la ausencia de vigilancia o de control por parte de cualquier persona física mencionada en el párrafo 1 haya permitido la comisión de las infracciones descritas en el párrafo 1 a

27411



través de una persona física que actúa bajo autorización de la persona jurídica.

3. La responsabilidad de la persona jurídica podrá resolverse en sede penal, civil o administrativa, dependiendo de los principios jurídicos propios del Estado.



4. Esta responsabilidad se establecerá sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido la infracción.

Artículo 13 - Sanciones y medidas

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para permitir que las infracciones penales establecidas en los artículos 2 a 11 sean castigadas con sanciones efectivas, proporcionadas y disuasorias, incluidas las penas privativas de libertad.

2. Las Partes velarán para que las personas jurídicas que hayan sido declaradas responsables según lo dispuesto en el artículo 12 sean objeto de sanciones o medidas penales o no penales efectivas, proporcionadas y disuasorias, incluidas las sanciones pecuniarias.

Sección 2 - Derecho procesal

Título 1 - Disposiciones comunes

Artículo 14 - Ámbito de aplicación de las medidas de derecho procesal

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para instaurar los poderes y procedimientos previstos en la presente sección a los efectos de investigación o de procedimientos penales específicos.

2. Salvo disposición en contrario, prevista en el artículo 21, las Partes podrán aplicar los poderes y procedimientos mencionados en el párrafo 1:

- a. a las infracciones penales establecidas en los artículos 2 a 11 del presente Convenio;
- b. a cualquier otra infracción penal cometida a través de un sistema informático; y
- c. a la recopilación de pruebas electrónicas de cualquier infracción penal.

3. a. Las Partes podrán reservarse el derecho de aplicar la medida mencionada en el artículo 20 a las infracciones especificadas en sus reservas, siempre que el número de dichas infracciones no supere el de



[Handwritten signature]

[Handwritten signature]

[Handwritten signature]
ES GOBIERNO

aquellas a las que se aplica la medida mencionada en el artículo 21. Las Partes tratarán de limitar tal reserva de modo que se permita la aplicación lo más amplia posible de la medida mencionada en el artículo 20.

b. Cuando un Estado, en razón de las restricciones impuestas por su legislación vigente en el momento de la adopción del presente Convenio, no esté en condiciones de aplicar las medidas descritas en los artículos 20 y 21 a las comunicaciones transmitidas en un sistema informático de un prestador de servicios que

i. es utilizado en beneficio de un grupo de usuarios cerrado, y

ii. no emplea las redes públicas de telecomunicación y no está conectado a otro sistema informático, público o privado, ese Estado podrá reservarse el derecho de no aplicar dichas medidas a tales comunicaciones. Los Estados tratarán de limitar tal reserva de modo que se permita la aplicación lo más amplia posible de las medidas mencionadas en los artículos 20 y 21.

Artículo 15 – Condiciones y garantías

1. Las Partes velarán para que la instauración, puesta en funcionamiento y aplicación de los poderes y procedimientos previstos en la presente sección se sometan a las condiciones y garantías dispuestas en su derecho interno, que debe asegurar una protección adecuada de los derechos del hombre y de las libertades y, en particular, de los derechos derivados de las obligaciones que haya asumido en aplicación del Convenio para la protección de los derechos humanos y libertades fundamentales del Consejo de Europa (1950) y del Pacto internacional de derechos civiles y políticos de Naciones Unidas (1966) o de otros instrumentos internacionales relativos a los derechos del hombre, y que debe integrar el principio de proporcionalidad.

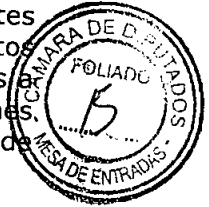
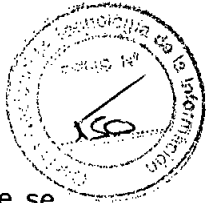
2. Cuando ello sea posible, en atención a la naturaleza del poder o del procedimiento de que se trate, dichas condiciones y garantías incluirán, entre otras, la supervisión judicial u otras formas de supervisión independiente, la motivación justificante de la aplicación, la limitación del ámbito de aplicación y la duración del poder o del procedimiento en cuestión.

3. Las Partes examinarán la repercusión de los poderes y procedimientos de esta Sección sobre los derechos, responsabilidades e intereses legítimos de terceros, en la medida que sea consistente con el interés público (y), en particular (, de) una correcta administración de justicia.

Título 2 – Conservación inmediata de datos informáticos almacenados

X

Artículo 16 – Conservación inmediata de datos informáticos almacenados



1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para permitir a sus autoridades competentes ordenar o imponer de otro modo la conservación inmediata de datos electrónicos especificados, incluidos los datos de tráfico, almacenados a través de un sistema informático, especialmente cuando hayan razones para pensar que son particularmente susceptibles de pérdida o de modificación.

2. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar a una persona a conservar y proteger la integridad de los datos - que se encuentran en su poder o bajo su control y respecto de los cuales exista un mandato previo de conservación en aplicación del párrafo precedente - durante el tiempo necesario, hasta un máximo de 90 días, para permitir a las autoridades competentes obtener su comunicación. Los Estados podrán prever que dicho mandato sea renovado posteriormente.

3. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar al responsable de los datos o a otra persona encargada de conservarlos a mantener en secreto la puesta en ejecución de dichos procedimientos durante el tiempo previsto por su derecho interno.

4. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.

X Artículo 17 - Conservación y divulgación inmediata de los datos de tráfico

1. A fin de asegurar la conservación de los datos de tráfico, en aplicación del artículo 16, las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para:

a. procurar la conservación inmediata de los datos de tráfico, cuando uno o más prestadores de servicio hayan participado en la transmisión de dicha comunicación; y

b. asegurar la comunicación inmediata a la autoridad competente del Estado, o a una persona designada por dicha autoridad, de datos de tráfico suficientes para permitir la identificación de los prestadores de servicio y de la vía por la que la comunicación se ha transmitido.

2. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.

Título 3 - Mandato de comunicación

Artículo 18 - Mandato de comunicación



[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

ES COPIA FIEL

CH
CA
PLA
PC

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para ordenar:

a. a una persona presente en su territorio que comunique los datos informáticos especificados, en posesión o bajo el control de dicha persona, y almacenados en un sistema informático o en un soporte de almacenaje informático; y

b. a un prestador de servicios que ofrezca sus prestaciones en el territorio del Estado firmante, que comunique los datos en su poder o bajo su control relativos a los abonados y que conciernen a tales servicios;

2. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.

3. A los efectos del presente artículo, la expresión «datos relativos a los abonados» designa cualquier información, expresada en datos informáticos o de cualquier otro modo, poseída por un prestador de servicio y que se refiere a los abonados de sus servicios, así como a los datos de tráfico o relativos al contenido, y que permite establecer:

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

b. la identidad, la dirección postal o geográfica y el número de teléfono del abonado o cualquier otro número de acceso, los datos relativos a la facturación y el pago; disponibles por razón de un contrato o de un alquiler de servicio;

c. cualquier otra información relativa al lugar donde se ubican los equipos de comunicación, disponible por razón de un contrato o de un alquiler de servicio.

Título 4 – Registro y decomiso de datos informáticos almacenados

X

Artículo 19 – Registro y decomiso de datos informáticos almacenados

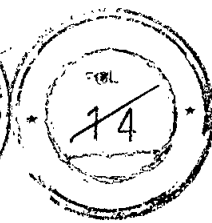
1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para registrar o acceder de un modo similar:

a. a un sistema informático o a una parte del mismo, así como a los datos informáticos que están almacenados; y

b. a un soporte de almacenamiento que permita contener datos informáticos

en su territorio.

27411



2. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para procurar que, cuando sus autoridades registren o accedan de un modo similar a un sistema informático específico o a una parte del mismo, conforme al párrafo 1 (a), 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, dichas autoridades estén en condiciones de ampliar inmediatamente el registro o el acceso y extenderlo al otro sistema.

3. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para decomisar u obtener de un modo similar los datos informáticos cuyo acceso haya sido realizado en aplicación de los párrafos 1 o 2. Estas medidas incluyen las prerrogativas siguientes:

- a. decomisar u obtener de un modo similar un sistema informático o una parte del mismo o un soporte de almacenaje 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 retirar los datos informáticos del sistema informático consultado.

4. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para ordenar a cualquier persona, que conozca el funcionamiento de un sistema informático o las medidas aplicadas para proteger los datos informáticos que contiene, que proporcione todas las informaciones razonablemente necesarias, para permitir la aplicación de las medidas previstas en los párrafos 1 y 2.

5. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.

Título 5 - Recopilación en tiempo real de datos informáticos

Artículo 20 - Recopilación en tiempo real de datos informáticos

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes para:

- a. recopilar o grabar mediante la aplicación de medios técnicos existentes en su territorio;



[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

ES COPIA FIEL

MA INSC

b. obligar a un prestador de servicios, en el ámbito de sus capacidades técnicas existentes, a

i. recopilar o grabar mediante la aplicación de medios técnicos existentes en su territorio, o

ii. prestar a las autoridades competentes su colaboración y su asistencia para recopilar o grabar, en tiempo real, los datos de tráfico asociados a comunicaciones específicas transmitidas en su territorio a través de un sistema informático.

2. Cuando un Estado, en razón de los principios establecidos en su ordenamiento jurídico interno, no pueda adoptar las medidas enunciadas en el párrafo 1 (a), podrá, en su lugar, adoptar otras medidas legislativas o de otro tipo que estime necesarias para asegurar la recopilación o la grabación en tiempo real de los datos de tráfico asociados a comunicaciones específicas transmitidas en su territorio mediante la aplicación de medios técnicos existentes en ese territorio.

3. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar a un prestador de servicios a mantener en secreto la adopción de las medidas previstas en el presente artículo, así como cualquier información al respecto.

4. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.

Artículo 21 - Interceptación de datos relativos al contenido

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias a fin de habilitar a sus autoridades competentes respecto a infracciones consideradas graves conforme a su derecho interno para:

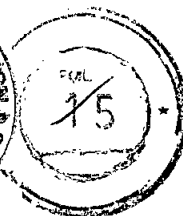
a. recopilar o grabar mediante la aplicación de medios técnicos existentes en su territorio; y

b. obligar a un prestador de servicios, en el ámbito de sus capacidades técnicas existentes, a

i. recopilar o grabar mediante la aplicación de medios técnicos existentes en su territorio, o

ii. prestar a las autoridades competentes su colaboración y su asistencia para recopilar o grabar,

en tiempo real, los datos relativos al contenido de concretas comunicaciones en su territorio, transmitidas a través de un sistema informático.



2. Cuando un Estado, en razón de los principios establecidos en su ordenamiento jurídico interno, no pueda adoptar las medidas enunciadas en el párrafo 1 (a), podrá, en su lugar, adoptar otras medidas legislativas o de otro tipo que estime necesarias para asegurar la recopilación o la grabación en tiempo real de los datos relativos al contenido de concretas comunicaciones transmitidas en su territorio mediante la aplicación de medios técnicos existentes en ese territorio.

3. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para obligar a un prestador de servicios a mantener en secreto la adopción de las medidas previstas en el presente artículo, así como cualquier información al respecto.

4. Los poderes y procedimientos mencionados en el presente artículo deben quedar sometidos a los artículos 14 y 15.

Sección 3 - Competencia

Artículo 22 - Competencia

1. Las Partes adoptarán las medidas legislativas o de otro tipo que se estimen necesarias para atribuirse la competencia respecto a cualquier infracción penal establecida en los artículos 2 a 11 del presente Convenio, cuando la infracción se haya cometido:

- a. en su territorio;
- b. a bordo de una nave que enarbole el pabellón de ese Estado;
- c. a bordo de una aeronave inmatriculada en ese Estado;
- d. por uno de sus súbditos, si la infracción es punible penalmente en el lugar donde se ha cometido o si la infracción no pertenece a la competencia territorial de ningún Estado.

2. Las Partes podrán reservarse el derecho de no aplicar, o de aplicar sólo en ciertos casos o condiciones específicas, las reglas de competencia definidas en los párrafos 1b a 1d del presente artículo o en cualquiera de las partes de esos párrafos.

3. Las Partes adoptarán las medidas que se estimen necesarias para atribuirse la competencia respecto de cualquier infracción mencionada en el artículo 24, párrafo 1 del presente Convenio, cuando el presunto autor de la misma se halle en su territorio y no pueda ser extraditado a otro Estado por razón de la nacionalidad, después de una demanda de extradición.

4. El presente Convenio no excluye ninguna competencia penal ejercida por un Estado conforme a su derecho interno.



ES COPIA FIEL

5. Cuando varios Estados reivindiquen una competencia respecto a una infracción descrita en el presente Convenio, los Estados implicados se reunirán, cuando ello sea oportuno, a fin de decidir cuál de ellos está en mejores condiciones para ejercer la persecución.

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 con arreglo a lo dispuesto en el presente capítulo, aplicando para ello los instrumentos internacionales relativos a la cooperación internacional en materia penal, acuerdos basados en la legislación uniforme o recíproca y en su propio derecho nacional, de la forma más amplia posible, con la finalidad de investigar los procedimientos concernientes a infracciones penales vinculadas a sistemas y datos informáticos o para recoger pruebas electrónicas de una infracción penal.

Título 2 – Principios relativos a la extradición

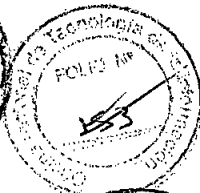
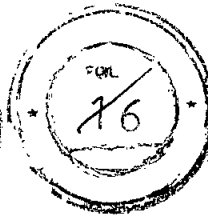
Artículo 24 – Extradición

1. a. El presente artículo se aplicará a la extradición por alguna de las infracciones definidas en los artículos 2 a 11 del presente Convenio, siempre que éstas resulten punibles por la legislación de los dos Estados implicados y tengan prevista una pena privativa de libertad de una duración mínima de un año.

b. Aquellos Estados que tengan prevista una pena mínima distinta, derivada de un tratado de extradición aplicable a dos o más Estados, comprendido en la Convención Europea de Extradición (STE nº 24), o de un acuerdo basado en la legislación uniforme o recíproca, aplicarán la pena mínima prevista en esos tratados o acuerdos.

2. Las infracciones penales previstas en el apartado 1 del presente artículo podrán dar lugar a extradición si entre los dos Estados existe un tratado de extradición. Las Partes se comprometerán a incluirlas como tales infracciones susceptibles de dar lugar a extradición en todos los tratados de extradición que puedan suscribir.

3. Si un Estado condiciona la extradición a la existencia de un tratado y recibe una demanda de extradición de otro Estado con el que no ha suscrito tratado alguno de extradición, podrá considerar el presente Convenio fundamento jurídico suficiente para conceder la extradición por alguna de las infracciones penales previstas en el párrafo 1 del presente artículo.



4. Las Partes que no condicionen la extradición a la existencia de un tratado podrán llevar a cabo la extradición siempre que prevean como infracciones las previstas en el párrafo 1 del presente artículo.

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

6. Si es denegada la extradición por una infracción comprendida en el párrafo 1 del presente artículo, alegando la nacionalidad de la persona reclamada o la competencia para juzgar la infracción del Estado requerido, éste deberá someter el asunto - la demanda del Estado requirente - a sus autoridades competentes a fin de que éstas establezcan la competencia para perseguir el hecho e informen de la conclusión alcanzada al Estado requirente. Las autoridades en cuestión deberán adoptar la decisión y sustanciar el procedimiento del mismo modo que para el resto de infracciones de naturaleza semejante previstas en la legislación de ese Estado.

7. a. Las Partes deberán comunicar al Secretario General del Consejo de Europa, en el momento de la firma o del depósito del instrumento de ratificación, aceptación, aprobación o adhesión, el nombre y la dirección de las autoridades responsables del envío y de la recepción de una demanda de extradición o de arresto provisional, en caso de ausencia de tratado.

b. El Secretario General del Consejo de Europa creará y actualizará un registro de autoridades designadas por las Partes. Las Partes deberán garantizar la exactitud de los datos obrantes en el registro

Título 3 - Principios generales relativos a la colaboración ⁽⁸⁾

Artículo 25 - Principios generales relativos a la colaboración

1. Las Partes acordarán llevar a cabo una colaboración mutua lo más amplia posible al objeto de investigar los procedimientos concernientes a infracciones penales vinculadas a sistemas y datos informáticos o al de recoger pruebas electrónicas de una infracción penal.

2. Las Partes adoptarán las medidas legislativas o de otro tipo que estimen necesarias para dar cumplimiento a las obligaciones establecidas en los artículos 27 a 35.

3. Las Partes podrán, en caso de emergencia, formular una demanda de colaboración, a través de un medio de comunicación rápido, como el fax o el correo electrónico, procurando que esos medios ofrezcan las condiciones suficientes de seguridad y de autenticidad (encriptándose si fuera necesario) y con confirmación posterior de la misma si el Estado requerido lo exigiera. Si el Estado requerido lo acepta podrá responder por cualquiera de los medios rápidos de comunicación indicados.



x [Signature]

x [Signature]

x [Signature]

ES COPIA FIEL

4. Salvo disposición en contrario expresamente prevista en el presente capítulo, la colaboración estará sometida a las condiciones fijadas en el derecho interno del Estado requerido o en los tratados de colaboración aplicables y comprenderá los motivos por los que el Estado requerido puede negarse a colaborar. El Estado requerido no podrá ejercer su derecho a rehusar la colaboración en relación a las infracciones previstas en los artículos 2 a 11, alegando que la demanda se solicita respecto a una infracción que, según su criterio, tiene la consideración de fiscal.

5. Conforme a lo dispuesto en el presente capítulo, el Estado requerido estará autorizado a supeditar la colaboración a la exigencia de doble incriminación. Esa condición se entenderá cumplida si el comportamiento constitutivo de la infracción - en relación a la que se solicita la colaboración - se encuentra previsto en su derecho interno como infracción penal, resultando indiferente que éste no la encuadre en la misma categoría o que no la designe con la misma terminología.

Artículo 26 – Información espontánea

1. Las Partes podrán, dentro de los límites de su derecho interno y en ausencia de demanda previa, comunicar a otro Estado las informaciones obtenidas en el marco de investigaciones que puedan ayudar a la Parte destinataria a iniciar o a concluir satisfactoriamente las investigaciones o procedimientos relativos a las infracciones dispuestas en el presente Convenio, o a que dicha parte presente una demanda de las previstas en el presente capítulo.

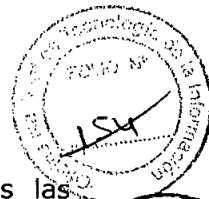
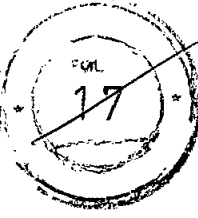
2. Antes de comunicar dicha información, ese Estado podrá solicitar que la información sea tratada de forma confidencial o que sea utilizada sólo en ciertas circunstancias. Si el Estado destinatario no pudiera acatar las condiciones impuestas, deberá informar al otro Estado, quien habrá de decidir si proporciona o no la información. Una vez aceptadas estas condiciones por el Estado destinatario, éste quedará obligado a su cumplimiento.

Título 4 – Procedimientos relativos a las demandas de asistencia en ausencia de acuerdo internacional aplicable

Artículo 27 – Procedimiento relativo a las demandas de colaboración en ausencia de acuerdo internacional aplicable

1. En ausencia de tratado o acuerdo en vigor de asistencia basado en la legislación uniforme o recíproca, serán aplicables los apartados 2 al 9 del presente artículo. Éstos no se aplicarán cuando exista un tratado, acuerdo o legislación sobre el particular, sin perjuicio de que las partes implicadas puedan decidir someterse, en todo o parte, a lo dispuesto en este artículo.

2. a. Las Partes designarán una o varias autoridades centrales encargadas de tramitar las demandas de colaboración, de ejecutarlas o



de transferirlas a las autoridades competentes para que éstas las ejecuten.

b. Las autoridades centrales se comunicarán directamente las unas con las otras.

c. Las Partes, en el momento de la firma o del depósito de sus instrumentos de ratificación, aceptación, de aprobación o de adhesión, comunicarán 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 actualizará un registro de autoridades designadas por las partes. Las Partes deberán garantizar la exactitud de los datos obrantes en el registro.

3. Las demandas de asistencia basadas en el presente artículo serán ejecutadas conforme al procedimiento especificado por el Estado requirente, siempre que resulte compatible con la legislación del Estado requerido.

4. Al margen de los motivos previstos en el artículo 15 párrafo 4 para denegar la asistencia, ésta podrá ser rechazada por el Estado requerido:

a. si la demanda se refiere a una infracción que el Estado requerido considera de naturaleza política o vinculada a una información de naturaleza política o;

b. si el Estado requerido estima que, de acceder a la colaboración, se pondría en peligro su soberanía, seguridad, orden público o otro interés esencial.

5. El Estado requerido podrá aplazar la ejecución de la demanda cuando ésta pueda perjudicar investigaciones o procedimientos en curso llevados a cabo por las autoridades nacionales.

6. Antes de denegar o retrasar la asistencia, el Estado requerido deberá examinar, tras consultar al Estado requirente, si es posible hacer frente a la demanda de forma parcial o si es posible establecer las reservas que estime necesarias.

7. El Estado requerido informará inmediatamente al Estado requirente del curso que pretende dar a la demanda de asistencia. De denegar o retrasar la tramitación de la demanda, el Estado requerido hará constar los motivos. Asimismo, dicho Estado deberá informar al Estado requirente sobre los motivos que hacen imposible, de ser así, la ejecución de la demanda o que retrasan sustancialmente su ejecución.

8. El Estado requirente podrá solicitar que el Estado requerido mantenga en secreto la propia existencia y objeto de la demanda



[Handwritten signatures]

ES COPIA FIEL

interpuesta al amparo de este capítulo, salvo en aquellos aspectos necesarios para la ejecución de la misma. Si el Estado requirente no pudiera hacer frente a la petición de confidencialidad, éste deberá informar inmediatamente al otro Estado, quien decidirá si la demanda, pese a ello, debe ser ejecutada.

9. a. En caso de urgencia, las autoridades judiciales del Estado requirente podrán dirigir directamente a las autoridades homólogas del Estado requerido las demandas de asistencia y las comunicaciones. En tales casos, se remitirá simultáneamente una copia a las autoridades del Estado requerido con el visado de la autoridad central del Estado requirente.

b. Todas las demandas o comunicaciones formuladas al amparo del presente párrafo podrán ser tramitadas a través de la Organización Internacional de Policía Criminal (INTERPOL).

c. Cuando una demanda haya sido formulada al amparo de la letra (a) del presente artículo, y la autoridad que le dio curso no sea la competente para ello, deberá transferir la demanda a la autoridad nacional competente y ésta informará directamente al Estado requerido.

d. Las demandas o comunicaciones realizadas al amparo del presente párrafo que no supongan la adopción de medidas coercitivas podrán ser tramitadas directamente por las autoridades del Estado requirente y las del Estado requerido.

e. Las Partes podrán informar 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, que, por motivos de eficacia, las demandas formuladas al amparo del presente párrafo deberán dirigirse directamente a su autoridad central.

Artículo 28 – Confidencialidad y restricciones de uso

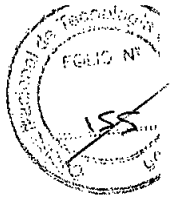
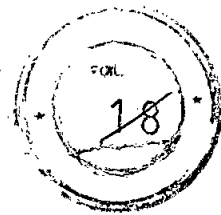
1. En ausencia de tratado o acuerdo en vigor de asistencia basados en la legislación uniforme o recíproca, será aplicable lo dispuesto en el presente artículo. Éste no se aplicará cuando exista un tratado, acuerdo o legislación sobre el particular, sin perjuicio de que las partes implicadas puedan decidir someterse, en todo o parte, a lo dispuesto en este artículo.

2. El Estado requerido podrá supeditar la comunicación de la información o del material requerido en la demanda al cumplimiento de las siguientes condiciones:

a. que se mantenga la confidencialidad sobre las mismas, siempre que la demanda corra el riesgo fracasar en ausencia de dicha condición; o

b. que éstas no sean utilizadas en investigaciones o procedimientos diversos a los establecidos en la demanda.

- 27411



3. Si el Estado requirente no pudiera satisfacer alguna de las condiciones establecidas en el apartado 2 del presente artículo, la otra parte informará al Estado requerido, el cual decidirá si la información debe ser proporcionada. Si el Estado requirente acepta esta condición, dicho Estado estará obligado por la misma.

4. Todo Estado parte que aporte información o material supeditado a alguna de las condiciones previstas en el apartado 2, podrá exigir de la otra parte la concreción de las condiciones de uso de la información o del material.

Sección 2 – Disposiciones específicas

Título 1 – Cooperación en materia de medidas cautelares

Artículo 29 – Conservación inmediata datos informáticos almacenados

1. Las Partes podrán ordenar o imponer de otro modo la conservación inmediata de datos almacenados en sistemas informáticos que se encuentren en su territorio, en relación a los cuales el Estado requirente tiene intención de presentar una demanda de asistencia para registrar o acceder de otro modo, decomisar u obtener por otro medio, o lograr la comunicación de dichos datos.

2. Una demanda de conservación formulada en aplicación del párrafo 1 deberá contener:

- a. la identificación de la autoridad que solicita la conservación;
- b. la infracción objeto de investigación con una breve exposición de los hechos vinculados a la misma;
- c. los datos informáticos almacenados que deben conservarse y su vinculación con la infracción;
- d. todas aquellas informaciones disponibles que permitan identificar al responsable de los datos informáticos almacenados o el emplazamiento de los sistemas informáticos;
- e. justificación de la necesidad de conservación; y
- f. la acreditación de que el Estado requirente está dispuesto a formular una demanda de asistencia para registrar o acceder de otro modo, decomisar u obtener por otro medio, o lograr la comunicación de dichos datos.

3. Después de recibir la demanda, el Estado requerido deberá adoptar las medidas necesarias para proceder sin dilaciones a la conservación de los datos solicitados, conforme a su derecho interno. Para hacer efectiva la demanda de conservación no resultará condición indispensable la doble incriminación.



x

x

ES COPIA FIEL

4. Si un Estado exige la doble incriminación como condición para atender a una demanda de asistencia para registrar o acceder de otro modo, decomisar u obtener por otro medio, o lograr la comunicación de dichos datos, por infracciones diversas a las establecidas en los artículos 2 a 11 del presente Convenio, podrá negarse a la demanda de conservación, al amparo del presente artículo, si tiene fundadas sospechas de que, en el momento de la comunicación de los datos, el otro Estado no cumplirá la exigencia de la doble incriminación.

5. Al margen de lo anterior, una demanda de conservación únicamente podrá ser denegada:

a. si la demanda se refiere a una infracción que el Estado requerido considera de naturaleza política o vinculada a una información de naturaleza política o;

b. si el Estado requerido estima que de acceder a la demanda se pondría en peligro su soberanía, su seguridad, orden público o otro interés esencial.

6. Cuando el Estado requerido considere que la simple conservación no será suficiente para garantizar la disponibilidad futura de los datos informáticos o que ésta podría comprometer la confidencialidad de la investigación o podría hacerla fracasar de otro modo, deberá informar inmediatamente al Estado requirente, quien decidirá la conveniencia de dar curso a la demanda.

7. Todas las conservaciones realizadas al amparo de una demanda de las previstas en el párrafo 1 serán válidas por un periodo máximo de 60 días, para permitir, en ese plazo de tiempo, al Estado requirente formular una demanda de asistencia para registrar o acceder de otro modo, decomisar u obtener por otro medio, o lograr la comunicación de dichos datos. Después de la recepción de la demanda, los datos informáticos deberán mantenerse hasta que ésta se resuelva.

Artículo 30 – Comunicación inmediata de los datos informáticos conservados

1. Si, en ejecución de una demanda de conservación de datos de tráfico relativos a una concreta comunicación al amparo del artículo 29, el Estado requerido descubriera que un prestador de servicios de otro Estado ha participado en la transmisión de la comunicación, comunicará inmediatamente al Estado requirente los datos informáticos de tráfico, con el fin de que éste identifique al prestador de servicios y la vía por la que la comunicación ha sido realizada.

2. La comunicación de datos informáticos de tráfico prevista en el párrafo 1 únicamente podrá ser denegada:

a. si la demanda se refiere a una infracción que el Estado requerido considera de naturaleza política o vinculada a una información de naturaleza política o;



b. si el Estado requerido estima que de acceder a la demanda se pondría en peligro su soberanía, su seguridad, orden público o otro interés esencial.

Título 2 - Asistencia en relación a los poderes de investigación



Artículo 31 - Asistencia concerniente al acceso a datos informáticos almacenados

1. Cualquier Estado podrá solicitar a otro el registro o acceso de otro modo, el decomiso u obtención por otro medio, o la comunicación de datos almacenados en un sistema informático que se encuentre en su territorio, incluidos los datos conservados conforme a lo dispuesto en el artículo 29.
2. El Estado requerido dará satisfacción a la demanda aplicando los instrumentos internacionales, convenios y la legislación mencionada en el artículo 23 siempre que no entre en contradicción con lo dispuesto en el presente capítulo.
3. La demanda deberá ser satisfecha lo más rápidamente posible en los siguientes casos:
 - a. cuando existan motivos para sospechar que los datos solicitados son particularmente vulnerables por existir riesgo de pérdida o modificación; o
 - b. cuando los instrumentos, convenios o legislación referida en el párrafo 2 prevean una cooperación rápida.

Artículo 32 - Acceso transfronterizo a los datos informáticos almacenados, con consentimiento o de libre acceso

Cualquier Estado podrá sin autorización de otro:

- a. acceder a los datos informáticos almacenados de libre acceso al público código abierto, independientemente de la localización geográfica de esos datos; o
- b. acceder a, o recibir a través de un sistema informático situado en su territorio, los datos informáticos almacenados situados en otro Estado, si se obtiene el consentimiento legal y voluntario de la persona autorizada para divulgarlos a través de ese sistema informático.

Artículo 33 - Asistencia para la recolección en tiempo real de datos de tráfico

1. Las Partes podrán acordar colaborar en la recolección, en tiempo real, de datos de tráfico, asociados a concretas comunicaciones llevadas a cabo en sus territorios, a través un sistema informático. Dicha colaboración se someterá a las condiciones y procedimientos previstos



Handwritten signatures and initials: 'x' followed by a signature, 'x' followed by another signature, and 'x' followed by a signature.

ES COPIA FIEL

SH
A
LAT.
> 01
LILIA
T 000
10
MAT. T.
INSCRIP. N

en el derecho interno, salvo que alguna de las partes se acoja a la reserva prevista en el párrafo 2.

2. Las Partes deberán acordar colaborar respecto a aquellas infracciones penales para las cuales la recolección en tiempo real de datos de tráfico se encuentra prevista en su derecho interno en situaciones análogas.

Artículo 34 – Asistencia en materia de interceptación de datos relativos al contenido

Las Partes podrán acordar colaborar, en la medida en que se encuentre previsto por tratados o leyes internas, en la recolección, y registro, en tiempo real, de datos relativos al contenido de concretas comunicaciones realizadas a través de sistemas informáticos.

Título 3 – Red 24/7

Artículo 35 – Red 24/7

1. Las Partes designarán 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 infracciones penales llevadas a cabo a través de sistemas y datos informáticos o en la recolección de pruebas electrónicas de una infracción penal. Esta asistencia comprenderá, si lo permite el derecho y la práctica interna, facilitar la aplicación directa de las siguientes medidas:

- a. aportación de consejos técnicos;
- b. conservación de datos según lo dispuesto en los artículos 29 y 30; y
- c. recolección de pruebas, aportación de información de carácter jurídico y localización de sospechosos.

2. a. Un mismo punto de contacto podrá ser coincidente para dos Estados, siguiendo para ello un procedimiento acelerado.

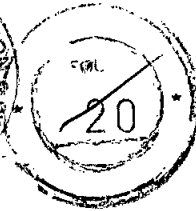
b. Si el punto de contacto designado por un Estado no depende de su autoridad o autoridades responsables de la colaboración internacional o de la extradición, deberá velarse para que ambas autoridades actúen coordinadamente mediante la adopción de un procedimiento acelerado.

3. Las Partes dispondrán de personal formado y dotado de equipamiento a fin de facilitar el funcionamiento de la red.

Capítulo IV – Cláusulas finales

Artículo 36 – Firma y entrada en vigor

27411



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 está sometido a ratificación, aceptación o aprobación. Los instrumentos de ratificación, aceptación o aprobación deberán ser entregados al Secretario General del Consejo de Europa.



3. El presente Convenio entrará en vigor el primer día del mes transcurridos tres meses desde que cinco Estados, de los cuales al menos tres deberán ser miembros del Consejo de Europa, presten su consentimiento a vincularse al Convenio, conforme a lo dispuesto en los párrafos 1 y 2.

4. Para todos los Estados que hayan prestado su consentimiento a vincularse al Convenio, éste entrará en vigor el primer día del mes transcurridos tres meses desde que hayan expresado su consentimiento, conforme a lo dispuesto en los párrafos 1 y 2.

Artículo 37 - Adhesión al Convenio

1. Después de entrar en vigor el presente Convenio, el Comité de Ministros del Consejo de Europa podrá, tras consultar a las Partes del Convenio y habiendo obtenido el asentimiento unánime de los mismos, invitar a todos los Estados no miembros del Consejo de Europa que no hayan participado en la elaboración del mismo a adherirse al Convenio. Esta decisión deberá tomarse mediante la mayoría prevista en el artículo 20.d del Estatuto del Consejo de Europa y el asentimiento unánime de los Estados Partes que tengan derecho a formar parte del Comité de Ministros.

2. Para todos aquellos Estados que se adhieran al Convenio conforme a lo previsto en el párrafo precedente, el Convenio entrará en vigor el primer día del mes transcurridos tres meses después del depósito del instrumento de adhesión ante el Secretario General del Consejo de Europa.

Artículo 38 - Aplicación territorial

1. Las Partes podrán, en el momento de la firma o del depósito del instrumento de ratificación, aceptación, aprobación o adhesión, designar el territorio al que resultará aplicable el presente Convenio.

2. Las Partes podrán, en cualquier momento, a través de una declaración dirigida al Secretario General del Consejo de Europa, extender la aplicación del presente Convenio a otros territorios diversos a los designados en la declaración. En tal caso, el Convenio entrará en vigor en dichos territorios el primer día del mes transcurridos tres meses desde la recepción de la declaración por el Secretario General.

3. Toda declaración realizada al amparo de los párrafos precedentes podrá ser retirada, en lo que concierne al territorio designado en la



x *[Handwritten signature]*

x *[Handwritten signature]*

[Handwritten signature]

[Handwritten signature]

ES COPIA FIEL

citada declaración, a través de una notificación dirigida al Secretario General del Consejo de Europa. El retracto surtirá efecto el primer día del mes transcurridos tres meses desde la recepción de la notificación por el Secretario General.

Artículo 39 – Efectos del Convenio

1. El objeto del presente Convenio es completar los tratados o acuerdos multilaterales o bilaterales existentes entre las partes, y comprende las disposiciones:

– del Convenio Europeo de extradición abierto a la firma el 13 de diciembre de 1957 en París (STE nº 24)

– del Convenio Europeo de Cooperación judicial en materia penal abierto a la firma el 20 de abril de 1959 en Estrasburgo (STE nº 30),

– del Protocolo Adicional del Convenio Europeo de Cooperación judicial en materia penal abierto a la firma el 17 de marzo de 1978 en Estrasburgo (STE nº 99).

2. Si dos o más Estados han concluido un acuerdo o un tratado relativo a la materia objeto de este Convenio o si han establecido de otro modo la relación entre ellos, o si lo hacen en el futuro, dispondrán igualmente de la facultad de aplicar el citado acuerdo o de establecer sus relaciones con base en el mismo, en lugar del presente Convenio. Siempre que los Estados hayan establecido sus relaciones concernientes a la materia objeto del presente Convenio de forma diversa, éstas deberán llevarse a cabo de forma compatible con los objetivos y principios del Convenio.

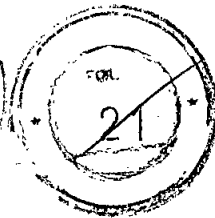
3. Lo dispuesto en el presente Convenio no afectará a otros derechos, restricciones, obligaciones y responsabilidades de los Estados.

Artículo 40 – Declaraciones

A través de una declaración escrita dirigida al Secretario General del Consejo de Europa, las Partes podrán, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, declarar que se reservan el derecho a exigir, llegado el caso, uno o varios elementos suplementarios de los dispuestos en los artículos 2, 3, 6 del párrafo 1 (b), 7, 9 párrafo 3 y 27 del párrafo 9 (e).

Artículo 41 – Cláusula federal

1. Un Estado federal podrá reservarse el derecho de desempeñar sus obligaciones, en los términos previstos en el capítulo II del presente Convenio, en la medida en que éstas sean compatibles con los principios que presiden las relaciones entre el gobierno central y los Estados federados u otros territorios análogos, siempre que se garantice la cooperación en los términos previstos en el capítulo III.



2. Un Estado federal no podrá hacer uso de la reserva adoptada según lo dispuesto en el párrafo 1 para excluir o disminuir de forma substancial las obligaciones contraídas en virtud del capítulo II. En todo caso, el Estado federal deberá dotarse de los medios necesarios para dar cumplimiento a las medidas previstas en el citado capítulo.

3. En todo lo que concierne a las disposiciones de este Convenio cuya aplicación dimana de la competencia de cada uno de los Estados federados u otras entidades territoriales análogas, que no están, en virtud del sistema constitucional de la federación, obligados a adoptar medidas legislativas, el gobierno central pondrá, con la aprobación de éstos, en conocimiento de las autoridades competentes de los Estados federados la necesidad de adoptar las citadas medidas animándolos a que las ejecuten.

Artículo 42 – Reservas

Los Estados podrán, a través de una notificación escrita dirigida al Secretario del Consejo de Europa, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o de adhesión, declarar que invocan la reserva o reservas previstas en el art. 4, párrafo 2, artículo 6, párrafo 3, artículo 9, párrafo 4, artículo 10, párrafo 3, artículo 11, párrafo 3, artículo 14, párrafo 3, artículo 22, párrafo 2, artículo 29, párrafo 4 y en el artículo 41, párrafo 1. No podrá realizarse ninguna otra reserva diversa a las indicadas.

Artículo 43 – Mantenimiento y retirada de las reservas

1. El Estado que haya formulado una reserva conforme a lo dispuesto en el artículo 42 podrá retirarla total o parcialmente notificando tal extremo al Secretario General. La retirada se hará efectiva en la fecha de recepción por el Secretario General de la notificación. Si en la notificación se hiciera constar que la reserva deberá tener efecto en una determinada fecha, ello se hará efectivo siempre que sea posterior a la recepción por el Secretario General de la notificación.

2. El Estado que haya formulado una reserva conforme a lo dispuesto en el artículo 42, podrá retirarla total o parcialmente siempre que lo permitan las circunstancias.

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

Artículo 44 – Enmiendas

1. Las enmiendas al presente Convenio podrán ser propuestas por las Partes, y deberán ser comunicadas al Secretario General del Consejo de Europa, a los Estados miembros del Consejo de Europa, a los Estados no miembros del Consejo de Europa que hayan tomado parte en la elaboración del Convenio así como a los Estados que se hayan adherido



[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

ES COPIA FIEL

o que hayan sido invitados a adherirse conforme a lo dispuesto en el artículo 37.

2. Las enmiendas propuestas por uno de los Estados deberán ser comunicadas al Comité europeo para los problemas criminales (CDPC), quien deberá informar al Comité de Ministros sobre las mismas.

3. El Comité de Ministros examinará la enmienda propuesta y el informe del Comité europeo para los problemas criminales (CDPC) y, después de consultar con los Estados no miembros y partes del Convenio, podrá adoptar la enmienda.

4. El texto de la enmienda adoptado por el Comité de Ministros, conforme a lo dispuesto en el párrafo 3 del presente artículo, deberá comunicarse a los Estados para su aceptación.

5. Las enmiendas adoptadas conforme al párrafo 3 del presente artículo entrarán en vigor el trigésimo día después del que los Estados hayan informado al Secretario General de su aceptación.

Artículo 45 – Reglamento de controversia

1. El Comité europeo para los problemas criminales (CDPC) está obligado a informar de la interpretación y aplicación del presente Convenio.

2. En caso de diferencias entre los Estados sobre la interpretación o aplicación del presente Convenio, los Estados intentarán adoptar un reglamento de diferencia a través de la negociación o de cualquier otro medio pacífico, con el compromiso de someter la controversia al Comité europeo para los problemas criminales, a un tribunal arbitral que tomará las decisiones que los Estados le sometan, o a la Corte internacional de justicia, a partir de un acuerdo adoptado por los Estados en litigio.

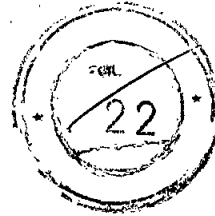
Artículo 46 – Reuniones de los Estados

1. Las Partes deberán reunirse periódicamente a fin de facilitar:

a. el uso y el efectivo cumplimiento del presente Convenio, la identificación de los problemas en esta materia, así como el efecto de las declaraciones o reservas formuladas conforme al presente Convenio;

b. el intercambio de información sobre novedades jurídicas, políticas o técnicas referentes al cibercrimen y recolección de pruebas electrónicas;

c. el examen sobre la posible reforma del Convenio.



2. El Comité europeo para los problemas criminales (CDPC) deberá estar al corriente de las reuniones llevadas a cabo al amparo del párrafo 1.

3. El Comité europeo para los problemas criminales (CDPC) deberá facilitar las reuniones previstas en el párrafo 1 y adoptar las medidas necesarias para ayudar a los Estados a completar o modificar el Convenio. No más tarde de tres años a contar desde la entrada en vigor del presente Convenio, el Comité europeo para los problemas criminales (CDPC) procederá, en cooperación con los Estados, a un examen conjunto de las disposiciones de la Convención y propondrá, en su caso, las modificaciones pertinentes.

4. Salvo que el Consejo de Europa los asuma, los gastos que ocasione la aplicación de las disposiciones del párrafo 1 deberán ser soportados por los Estados del modo que ellos mismos determinen.

5. Las Partes serán asistidas por el Secretariado del Consejo de Europa para llevar a cabo las funciones relativas a este artículo

Artículo 47 - Denuncia

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

2. La denuncia entrará en vigor el primer día del mes transcurridos tres meses desde la recepción de la notificación por el Secretario General.

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 tomado parte en la elaboración del presente Convenio, así como a cualquier Estado que se haya adherido o que haya sido invitado a adherirse:

a. cualquier firma;

b. el depósito de cualquier instrumento de ratificación, aceptación, aprobación o adhesión;

c. la fecha de entrada en vigor del presente Convenio según lo dispuesto en los artículos 36 y 37;

d. cualquier declaración realizada bajo el Artículo 40 y 41 o cualquier reserva formulada en virtud del artículo 42;

e. cualquier acto, notificación o comunicación referida al presente Convenio.



* *[Handwritten signature]*

* *[Handwritten signature]*

ES COPIA FIEL

[Handwritten signature]

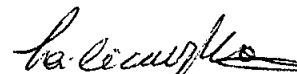
JH
CA
LA
PO

En vista de lo cual, los abajo firmantes, debidamente autorizados al efecto, han firmado el presente Convenio.

Hecho en Budapest, el 23 noviembre 2001, en francés y en inglés, ambos textos con el mismo valor, y en un solo ejemplar que será depositado 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.

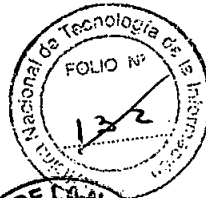
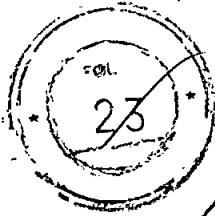
-
- (1) El Convenio recoge, en la versión francesa, la expresión «fournisseur de services», cuya traducción literal sería la de «proveedor de servicios». En la presente traducción, se ha optado por emplear el término «prestador de servicios», en la línea seguida por la Directiva 2000/31 y el Proyecto de LSSI, como concepto o categoría omnicomprendiva que hace referencia a aquellos sujetos que desempeñan, profesionalmente, la actividad de prestación y gestión de accesos y servicios en Internet.
- (2) También suele emplearse, para aludir a este tipo de datos, el término «datos de tránsito».
- (3) El Convenio emplea el término «intentionnel». Sin embargo, en este caso, se ha preferido utilizar el vocablo «doloso» por corresponderse mejor con la categoría jurídico-penal propia del derecho español.
- (4) El original en francés rubrica este ciberdelito como «Abus de dispositifs», lo que ha dado lugar a una traducción literal del mismo como «Abuso de dispositivos», expresión a la que, sin embargo, se ha preferido renunciar, por estimarse más precisa la empleada en texto.
- (5) La interpretación de este último inciso suscita algunos interrogantes. De la literalidad del precepto podría deducirse que la referencia «elementos» debe circunscribirse a los propios mecanismos o instrumentos aludidos en el precepto. Sin embargo, también sería posible inferir que el término «elementos» alude a «ánimos» o «intenciones», de modo similar a lo exigido en relación a otros delitos. Esta ambigüedad es resuelta a favor de la primera de las interpretaciones indicadas, por el Rapport explicatif del Convenio, en su parágrafo 75.
- (6) Esta descripción se corresponde con la denominada «pornografía técnica».
- (7) Esta descripción se corresponde con la denominada «simulada» o «pseudopornografía».
- (8) El Convenio emplea el término «entraide», cuya traducción en español resulta multívoca. Entre las distintas acepciones que puede asumir el vocablo (ayuda mutua, asistencia, colaboración), se han utilizado, de modo indistinto, «asistencia» y «colaboración».

Es traducción fiel del idioma inglés al idioma español del documento adjunto y al cual me remito, en la Ciudad Autónoma de Buenos Aires, a los 25 días del mes de octubre de 2012.



LILIANA B. BOSCH
TRADUCTORA PÚBLICA
IDIOMA INGLÉS
MAT. Tº 1 - Fº 46 LA PLATA
INSCRIP. Nº CTPIPBA LP 0068

P. 3153/16



COUNCIL OF EUROPE / CONSEIL DE L'EUROPE

European Treaty Series - No. 185



27411



CONVENTION ON CYBERCRIME

Budapest, 23.XI.2001



[Handwritten signature]

[Handwritten signature]

ES COPIA FIEL

[Handwritten signature]

MA INSCP

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia*, by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

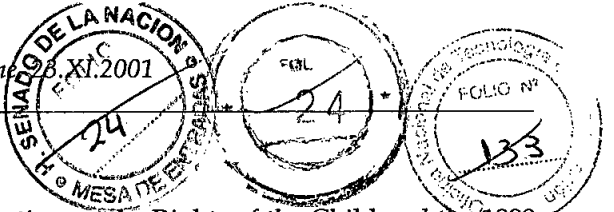
Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;

Mindful of the need to ensure a proper balance between the interests of law enforcement and respect for fundamental human rights as enshrined in the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights and other applicable international human rights treaties, which reaffirm the right of everyone to hold opinions without interference, as well as the right to freedom of expression, including the freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers, and the rights concerning the respect for privacy;

Mindful also of the right to the protection of personal data, as conferred, for example, by the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data;

- 27411



Considering the 1989 United Nations Convention on the Rights of the Child and the 1999 International Labour Organization Worst Forms of Child Labour Convention;

Taking into account the existing Council of Europe conventions on co-operation in the penal field, as well as similar treaties which exist between Council of Europe member States and other States, and stressing that the present Convention is intended to supplement those conventions in order to make criminal investigations and proceedings concerning criminal offences related to computer systems and data more effective and to enable the collection of evidence in electronic form of a criminal offence;



Welcoming recent developments which further advance international understanding and co-operation in combating cybercrime, including action taken by the United Nations, the OECD, the European Union and the G8;

Recalling Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, No. R (88) 2 on piracy in the field of copyright and neighbouring rights, No. R (87) 15 regulating the use of personal data in the police sector, No. R (95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, as well as No. R (89) 9 on computer-related crime providing guidelines for national legislatures concerning the definition of certain computer crimes and No. R (95) 13 concerning problems of criminal procedural law connected with information technology;

Having regard to Resolution No. 1 adopted by the European Ministers of Justice at their 21st Conference (Prague, 10 and 11 June 1997), which recommended that the Committee of Ministers support the work on cybercrime carried out by the European Committee on Crime Problems (CDPC) in order to bring domestic criminal law provisions closer to each other and enable the use of effective means of investigation into such offences, as well as to Resolution No. 3 adopted at the 23rd Conference of the European Ministers of Justice (London, 8 and 9 June 2000), which encouraged the negotiating parties to pursue their efforts with a view to finding appropriate solutions to enable the largest possible number of States to become parties to the Convention and acknowledged the need for a swift and efficient system of international co-operation, which duly takes into account the specific requirements of the fight against cybercrime;

Having also regard to the Action Plan adopted by the Heads of State and Government of the Council of Europe on the occasion of their Second Summit (Strasbourg, 10 and 11 October 1997), to seek common responses to the development of the new information technologies based on the standards and values of the Council of Europe;

Have agreed as follows:



Handwritten signatures and initials, including a large 'BL' signature, a signature with an 'x' mark, and another signature at the bottom.

ES COPIA FIEL

Chapter I – Use of terms

Article 1 – Definitions

For the purposes of this Convention:

- a "computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data;
- b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;
- c "service provider" means:
 - i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
 - ii any other entity that processes or stores computer data on behalf of such communication service or users of such service;
- d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.

Chapter II – Measures to be taken at the national level

Section 1 – Substantive criminal law

Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems

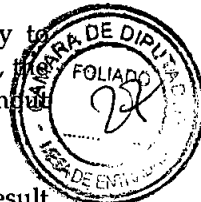
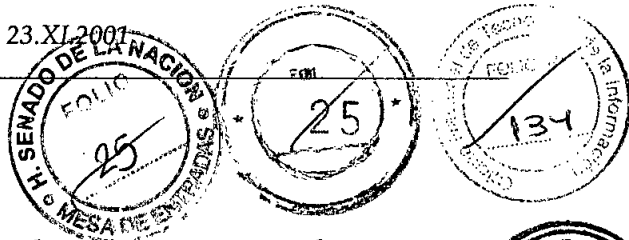
Article 2 – Illegal access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

- 27411



Article 4 - Data interference

- 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, damaging, deletion, deterioration, alteration or suppression of computer data without right.
- 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Article 5 - System interference

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

Article 6 - Misuse of devices

- 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:
 - a the production, sale, procurement for use, import, distribution or otherwise making available of:
 - i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;
 - ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,
 with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and
 - b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.
- 2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.
- 3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.



Handwritten signatures and initials, including a large signature on the left and several smaller ones on the right.

ES COPIA FIEL

*Title 2 – Computer-related offences***Article 7 – Computer-related forgery**

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

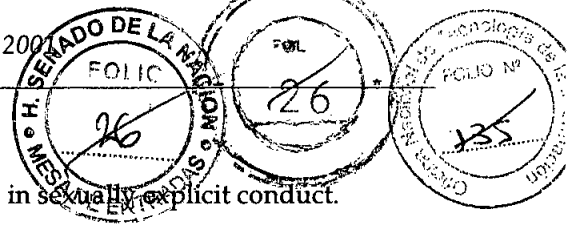
- a any input, alteration, deletion or suppression of computer data;
- b any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

*Title 3 – Content-related offences***Article 9 – Offences related to child pornography**

- 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:
 - a producing child pornography for the purpose of its distribution through a computer system;
 - b offering or making available child pornography through a computer system;
 - c distributing or transmitting child pornography through a computer system;
 - d procuring child pornography through a computer system for oneself or for another person;
 - e possessing child pornography in a computer system or on a computer-data storage medium.
- 2 For the purpose of paragraph 1 above, the term “child pornography” shall include pornographic material that visually depicts:
 - a a minor engaged in sexually explicit conduct;
 - b a person appearing to be a minor engaged in sexually explicit conduct;

27411



c realistic images representing a minor engaged in sexually explicit conduct.

3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.



Title 4 - Offences related to infringements of copyright and related rights

Article 10 - Offences related to infringements of copyright and related rights

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

Title 5 - Ancillary liability and sanctions

Article 11 - Attempt and aiding or abetting

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.



Handwritten signature with an asterisk.

Handwritten signature.

Handwritten signature.

Handwritten signature and the text "ES COPIA FIEL".

- 3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

Article 12 – Corporate liability

- 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:
- a a power of representation of the legal person;
 - b an authority to take decisions on behalf of the legal person;
 - c an authority to exercise control within the legal person.
- 2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.
- 3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.
- 4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

Article 13 – Sanctions and measures

- 1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.
- 2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.

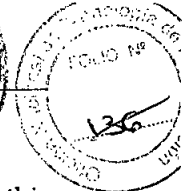
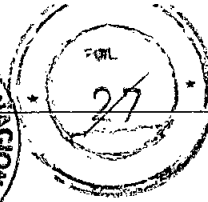
Section 2 – Procedural law

Title 1 – Common provisions

Article 14 – Scope of procedural provisions

- 1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.
- 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:

27411



- a the criminal offences established in accordance with Articles 2 through 11 of this Convention;
- b other criminal offences committed by means of a computer system; and
- c the collection of evidence in electronic form of a criminal offence.

3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.

b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:

- i is being operated for the benefit of a closed group of users, and
- ii does not employ public communications networks and is not connected with another computer system, whether public or private,

that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21.

Article 15 - Conditions and safeguards

1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia*, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

L
1
MAY
INSCR



Handwritten signatures and initials: BL, [unclear], [unclear], [unclear]

ES COPIA FIEL

*Title 2 – Expedited preservation of stored computer data***Article 16 – Expedited preservation of stored computer data**

- 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.
- 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.
- 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.
- 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

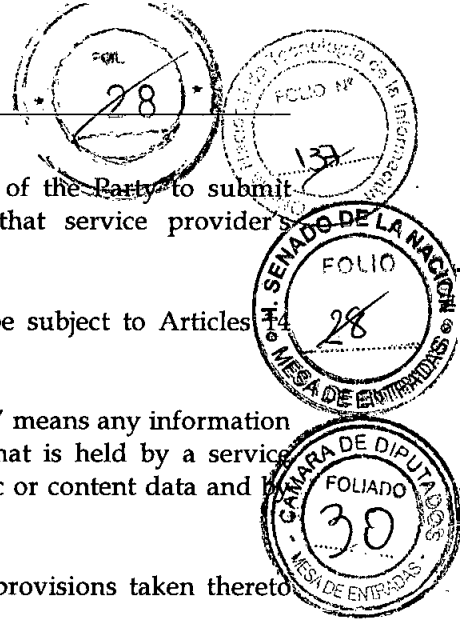
Article 17 – Expedited preservation and partial disclosure of traffic data

- 1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:
 - a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and
 - b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.
- 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

*Title 3 – Production order***Article 18 – Production order**

- 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:
 - a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

27411



- b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.
- 2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.
- 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and which can be established:
- the type of communication service used, the technical provisions taken thereto and the period of service;
 - the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
 - any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Title 4 - Search and seizure of stored computer data

Article 19 - Search and seizure of stored computer data

- 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:
- a computer system or part of it and computer data stored therein; and
 - a computer-data storage medium in which computer data may be stored
- in its territory.
- 2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.
- 3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:
- seize or similarly secure a computer system or part of it or a computer-data storage medium;
 - make and retain a copy of those computer data;



Handwritten signatures and initials, including a large stylized signature, a signature with a cross, and another signature with a cross.

ES COPIA FIEL

- c maintain the integrity of the relevant stored computer data;
 - d render inaccessible or remove those computer data in the accessed computer system.
- 4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.
- 5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Title 5 - Real-time collection of computer data

Article 20 - Real-time collection of traffic data

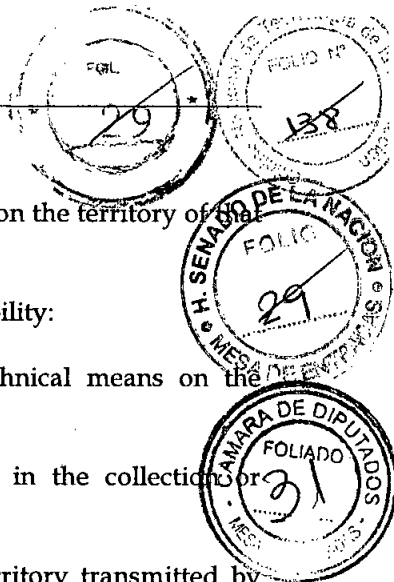
- 1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:
- a collect or record through the application of technical means on the territory of that Party, and
 - b compel a service provider, within its existing technical capability:
 - i to collect or record through the application of technical means on the territory of that Party; or
 - ii to co-operate and assist the competent authorities in the collection or recording of,
- traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.
- 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.

- 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.
- 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Article 21 - Interception of content data

- 1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:

- 27411



- a collect or record through the application of technical means on the territory of that Party, and
- b compel a service provider, within its existing technical capability:
 - i to collect or record through the application of technical means on the territory of that Party, or
 - ii to co-operate and assist the competent authorities in the collection or recording of,

content data, in real-time, of specified communications in its territory transmitted by means of a computer system.

- 2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.
- 3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.
- 4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

Section 3 - Jurisdiction

Article 22 - Jurisdiction

- 1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:
 - a in its territory; or
 - b on board a ship flying the flag of that Party; or
 - c on board an aircraft registered under the laws of that Party; or
 - d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.
- 2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.
- 3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.



Handwritten signatures and initials, including a large signature on the left and another on the right, with small 'x' marks next to them.

ES COPIA FIEL

- 4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.
- 5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Chapter III – International co-operation

Section 1 – General principles

Title 1 – General principles relating to international co-operation

Article 23 – General principles relating to international co-operation

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through the application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

Title 2 – Principles relating to extradition

Article 24 – Extradition

- 1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.
b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.
- 2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.
- 3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.
- 4 Parties that do not make extradition conditional on the existence of a treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

- 27411

- 5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.
- 6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.
- 7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.
- b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

Title 3 - General principles relating to mutual assistance

Article 25 - General principles relating to mutual assistance

- 1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.
- 2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.
- 3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.
- 4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.
- 5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.



* *[Handwritten signature]*

* *[Handwritten signature]*

* *[Handwritten signature]*

ES COPIA FIEL

Article 26 - Spontaneous information

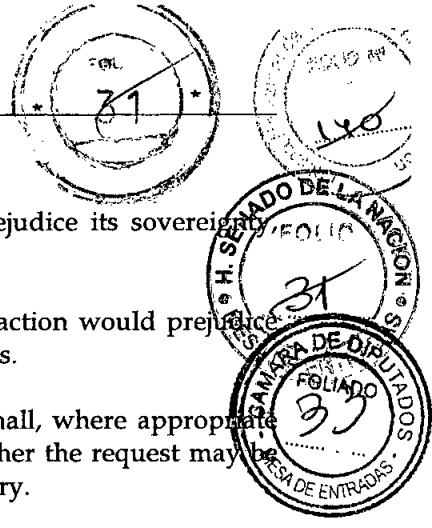
- 1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.
- 2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

*Title 4 - Procedures pertaining to mutual assistance requests
in the absence of applicable international agreements*

Article 27 - Procedures pertaining to mutual assistance requests in the absence of applicable international agreements

- 1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.
- 2
 - a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.
 - b The central authorities shall communicate directly with each other;
 - c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;
 - d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.
- 3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.
- 4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:
 - a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

27411



- b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.
- 5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.
- 6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.
- 7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.
- 8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.
- 9
 - a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.
 - b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).
 - c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.
 - d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.
 - e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Article 28 - Confidentiality and limitation on use

- 1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.
- 2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:



x [Signature]

x [Signature]

x [Signature]

M/ INBC

ES COPIA FIEL

- a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or
 - b not used for investigations or proceedings other than those stated in the request.
- 3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.
- 4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

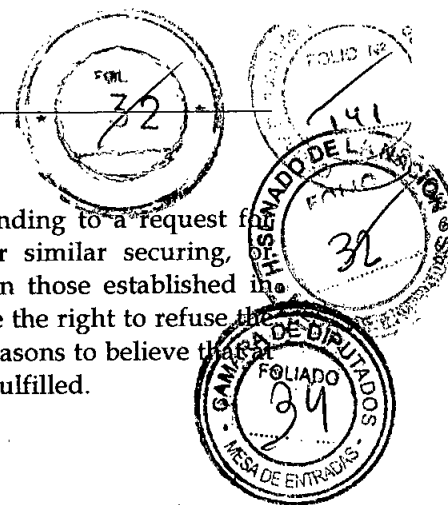
Section 2 – Specific provisions

Title 1 – Mutual assistance regarding provisional measures

Article 29 – Expedited preservation of stored computer data

- 1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.
- 2 A request for preservation made under paragraph 1 shall specify:
- a the authority seeking the preservation;
 - b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;
 - c the stored computer data to be preserved and its relationship to the offence;
 - d any available information identifying the custodian of the stored computer data or the location of the computer system;
 - e the necessity of the preservation; and
 - f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.
- 3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required as a condition to providing such preservation.

- 27411



4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5 In addition, a request for preservation may only be refused if:

- a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or
- b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

7 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

Article 30 - Expedited disclosure of preserved traffic data

1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

2 Disclosure of traffic data under paragraph 1 may only be withheld if:

- a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or
- b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

Title 2 - Mutual assistance regarding investigative powers

Article 31 - Mutual assistance regarding accessing of stored computer data

1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.



Handwritten signatures and initials, including a large signature on the left, a signature in the middle, and a signature on the right. A stamp at the bottom right reads 'ES COPIA FIEL'.

- 2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.
- 3 The request shall be responded to on an expedited basis where:
 - a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or
 - b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Article 32 – Trans-border access to stored computer data with consent or where publicly available

A Party may, without the authorisation of another Party:

- a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or
- b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

Article 33 – Mutual assistance in the real-time collection of traffic data

- 1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.
- 2 Each Party shall provide such assistance at least with respect to criminal offences for which real-time collection of traffic data would be available in a similar domestic case.

Article 34 – Mutual assistance regarding the interception of content data

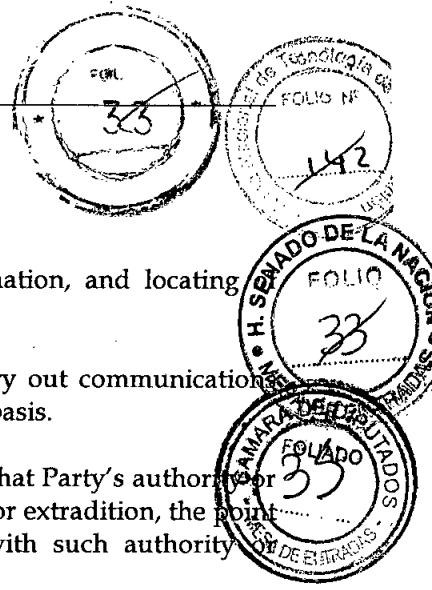
The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.

Title 3 – 24/7 Network

Article 35 – 24/7 Network

- 1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:
 - a the provision of technical advice;

27411



- b the preservation of data pursuant to Articles 29 and 30;
- c the collection of evidence, the provision of legal information, and locating suspects.
- 2 a A Party's point of contact shall have the capacity to carry out communication with the point of contact of another Party on an expedited basis.
- b If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.
- 3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

Chapter IV - Final provisions




Article 36 - Signature and entry into force



- 1 This Convention shall be open for signature by the member States of the Council of Europe and by non-member States which have participated in its elaboration.
- 2 This Convention is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.
- 3 This Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five States, including at least three member States of the Council of Europe, have expressed their consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.
- 4 In respect of any signatory State which subsequently expresses its consent to be bound by it, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the expression of its consent to be bound by the Convention in accordance with the provisions of paragraphs 1 and 2.

Article 37 - Accession to the Convention

- 1 After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.
- 2 In respect of any State acceding to the Convention under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.



* 
 * 
 * 

 * 
 * 

ES COPIA FIEL

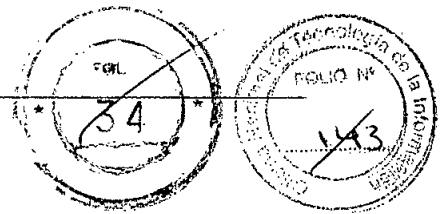
Article 38 – Territorial application

- 1 Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this Convention shall apply.
- 2 Any State may, at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this Convention to any other territory specified in the declaration. In respect of such territory the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of the declaration by the Secretary General.
- 3 Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General of the Council of Europe. The withdrawal shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of such notification by the Secretary General.

Article 39 – Effects of the Convention

- 1 The purpose of the present Convention is to supplement applicable multilateral or bilateral treaties or arrangements as between the Parties, including the provisions of:
 - the European Convention on Extradition, opened for signature in Paris, on 13 December 1957 (ETS No. 24);
 - the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 20 April 1959 (ETS No. 30);
 - the Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, opened for signature in Strasbourg, on 17 March 1978 (ETS No. 99).
- 2 If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or have otherwise established their relations on such matters, or should they in future do so, they shall also be entitled to apply that agreement or treaty or to regulate those relations accordingly. However, where Parties establish their relations in respect of the matters dealt with in the present Convention other than as regulated therein, they shall do so in a manner that is not inconsistent with the Convention's objectives and principles.
- 3 Nothing in this Convention shall affect other rights, restrictions, obligations and responsibilities of a Party.

27411



Article 40 - Declarations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the possibility of requiring additional elements as provided for under Articles 2, 3, 6 paragraph 1.b, paragraph 3, and 27, paragraph 9.e.

Article 41 - Federal clause

- 1 A federal State may reserve the right to assume obligations under Chapter II of this Convention consistent with its fundamental principles governing the relationship between its central government and constituent States or other similar territorial entities provided that it is still able to co-operate under Chapter III.
- 2 When making a reservation under paragraph 1, a federal State may not apply the terms of such reservation to exclude or substantially diminish its obligations to provide for measures set forth in Chapter II. Overall, it shall provide for a broad and effective law enforcement capability with respect to those measures.
- 3 With regard to the provisions of this Convention, the application of which comes under the jurisdiction of constituent States or other similar territorial entities, that are not obliged by the constitutional system of the federation to take legislative measures, the federal government shall inform the competent authorities of such States of the said provisions with its favourable opinion, encouraging them to take appropriate action to give them effect.

Article 42 - Reservations

By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.

Article 43 - Status and withdrawal of reservations

- 1 A Party that has made a reservation in accordance with Article 42 may wholly or partially withdraw it by means of a notification addressed to the Secretary General of the Council of Europe. Such withdrawal shall take effect on the date of receipt of such notification by the Secretary General. If the notification states that the withdrawal of a reservation is to take effect on a date specified therein, and such date is later than the date on which the notification is received by the Secretary General, the withdrawal shall take effect on such a later date.
- 2 A Party that has made a reservation as referred to in Article 42 shall withdraw such reservation, in whole or in part, as soon as circumstances so permit.
- 3 The Secretary General of the Council of Europe may periodically enquire with Parties that have made one or more reservations as referred to in Article 42 as to the prospects for withdrawing such reservation(s).



Handwritten signatures and initials, some with asterisks, indicating approval or authentication.

ES COPIA FIEL

Article 44 - Amendments

- 1 Amendments to this Convention may be proposed by any Party, and shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention as well as to any State which has acceded to, or has been invited to accede to, this Convention in accordance with the provisions of Article 37.
- 2 Any amendment proposed by a Party shall be communicated to the European Committee on Crime Problems (CDPC), which shall submit to the Committee of Ministers its opinion on that proposed amendment.
- 3 The Committee of Ministers shall consider the proposed amendment and the opinion submitted by the CDPC and, following consultation with the non-member States Parties to this Convention, may adopt the amendment.
- 4 The text of any amendment adopted by the Committee of Ministers in accordance with paragraph 3 of this article shall be forwarded to the Parties for acceptance.
- 5 Any amendment adopted in accordance with paragraph 3 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

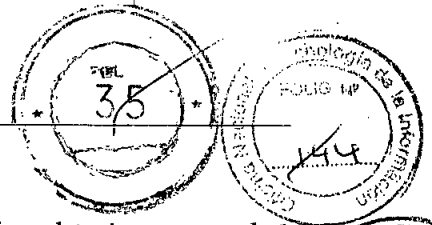
Article 45 - Settlement of disputes

- 1 The European Committee on Crime Problems (CDPC) shall be kept informed regarding the interpretation and application of this Convention.
- 2 In case of a dispute between Parties as to the interpretation or application of this Convention, they shall seek a settlement of the dispute through negotiation or any other peaceful means of their choice, including submission of the dispute to the CDPC, to an arbitral tribunal whose decisions shall be binding upon the Parties, or to the International Court of Justice, as agreed upon by the Parties concerned.

Article 46 - Consultations of the Parties

- 1 The Parties shall, as appropriate, consult periodically with a view to facilitating:
 - a the effective use and implementation of this Convention, including the identification of any problems thereof, as well as the effects of any declaration or reservation made under this Convention;
 - b the exchange of information on significant legal, policy or technological developments pertaining to cybercrime and the collection of evidence in electronic form;
 - c consideration of possible supplementation or amendment of the Convention.
- 2 The European Committee on Crime Problems (CDPC) shall be kept periodically informed regarding the result of consultations referred to in paragraph 1.

27411



- 3 The CDPC shall, as appropriate, facilitate the consultations referred to in paragraph 1 and take the measures necessary to assist the Parties in their efforts to supplement or amend the Convention. At the latest three years after the present Convention enters into force, the European Committee on Crime Problems (CDPC) shall, in co-operation with the Parties, conduct a review of all of the Convention's provisions and, if necessary, recommend any appropriate amendments.
- 4 Except where assumed by the Council of Europe, expenses incurred in carrying out the provisions of paragraph 1 shall be borne by the Parties in the manner to be determined by them.
- 5 The Parties shall be assisted by the Secretariat of the Council of Europe in carrying out their functions pursuant to this article.

Article 47 - Denunciation

- 1 Any Party may, at any time, denounce this Convention by means of a notification addressed to the Secretary General of the Council of Europe.
- 2 Such denunciation shall become effective on the first day of the month following the expiration of a period of three months after the date of receipt of the notification by the Secretary General.

Article 48 - Notification

The Secretary General of the Council of Europe shall notify the member States of the Council of Europe, the non-member States which have participated in the elaboration of this Convention as well as any State which has acceded to, or has been invited to accede to, this Convention of:

- a any signature;
- b the deposit of any instrument of ratification, acceptance, approval or accession;
- c any date of entry into force of this Convention in accordance with Articles 36 and 37;
- d any declaration made under Article 40 or reservation made in accordance with Article 42;
- e any other act, notification or communication relating to this Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Budapest, this 23rd day of November 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, and to any State invited to accede to it.



[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

[Handwritten signature]

ES COPIA FIEL

