Proyecto de Resolución Legislativa N° 2807/2018-PE

CONGRESO DE LA REPÚBLICA
ÁREA DE TRÁMITE DOCUMENTARIO
04 MAY 2018
RECIBIDO
Firma _____ Hora 16:50

"Decenio de la igualdad de oportunidades para mujeres y hombres"
"Año del Dialogo y la Reconciliación Nacional"

Lima, 2 de mayo de 2018

OFICIO N° 077–2018-PR

Señor
**LUIS GALARRETA VELARDE**
Presidente del Congreso de la República
Presente.-

Nos dirigimos a usted, señor Presidente del Congreso de la República, de conformidad con lo estipulado en los artículos 56° y 102°.3 de la Constitución Política del Perú, a fin de someter a consideración del Congreso de la República el Proyecto de Resolución Legislativa que aprueba el *"Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en la ciudad de Budapest.*

Con tal finalidad, acompañamos el expediente de sustento de la aludida Convención, que atiende los requisitos dispuestos en los artículos 75° y 76°.1.f) del Reglamento del Congreso de la República.

Sin otro particular, hacemos propicia la oportunidad para renovarle los sentimientos de nuestra consideración.

Atentamente,

MARTÍN ALBERTO VIZCARRA CORNEJO
Presidente de la República

NÉSTOR POPOLIZIO BARDALES
Ministro de Relaciones Exteriores

1

RU-127079

**CONGRESO DE LA REPÚBLICA**

**Lima, ....08.....de.....MAYO.....del 2018.....**

**Según la consulta realizada, de conformidad con el Artículo 77º del Reglamento del Congreso de la República: pase la Proposición Nº ....2807.... para su estudio y dictamen, a la (s) Comisión (es) de**

RELACIONES EXTERIORES.—

.....

.....

.....

.....

JOSÉ F. CEVASCO PIEDRA
Oficial Mayor
CONGRESO DE LA REPUBLICA

# *Proyecto de Resolución Legislativa*

*EL CONGRESO DE LA REPÚBLICA*

*Ha dado la Resolución Legislativa siguiente:*

## *RESOLUCIÓN LEGISLATIVA QUE APRUEBA EL CONVENIO SOBRE LA CIBERDELINCUENCIA*

***Artículo único. Objeto de la Resolución Legislativa***

*Apruébase el Convenio sobre la Ciberdelincuencia, adoptado en Budapest el 23 de noviembre de 2001, con las siguientes declaraciones y reservas:*

***DECLARACIONES***

a) De conformidad con lo dispuesto en el artículo 2 del Convenio sobre la Ciberdelincuencia, la República del Perú declara que su legislación exige que el delito de acceso ilícito se cometa infringiendo medidas de seguridad.

b) De conformidad con lo dispuesto en el artículo 3 del Convenio sobre la Ciberdelincuencia, la República del Perú declara que su legislación exige que el delito de interceptación ilícita se cometa con intención delictiva y que dicho delito puede cometerse en relación con un sistema informático conectado a otro sistema informático.

c) De conformidad con lo dispuesto en el artículo 7 del Convenio sobre la Ciberdelincuencia, la República del Perú declara que podrá exigir que exista una intención fraudulenta o delictiva similar, conforme a lo establecido en su derecho interno, para que las conductas descritas en dicho artículo generen responsabilidad penal.

d) De conformidad con lo establecido en el artículo 27, numeral 9, literal e) del Convenio sobre la Ciberdelincuencia, la República del Perú declara que, en aras de la eficacia, las solicitudes efectuadas en virtud de lo dispuesto en el numeral 9 del Convenio deberán dirigirse a su autoridad central.

***RESERVAS***

a) De conformidad con lo dispuesto en el párrafo 3 del artículo 6 del Convenio sobre la Ciberdelincuencia, la República del Perú se reserva el derecho de no aplicar el artículo 6, párrafo 1, literal b del Convenio.

b) De conformidad con el numeral 4 del artículo 9 del Convenio sobre la Ciberdelincuencia, la República del Perú considera que el bien jurídico tutelado en el derecho interno con respecto a la pornografía infantil es la libertad y/o indemnidad sexual de un menor, por lo que formula una reserva a los literales b) y c) del párrafo 2 del citado artículo, debido a que las conductas contempladas en dichas disposiciones no involucran la participación de un menor de edad.

c) Conforme al numeral 4 del artículo 29 del Convenio sobre la Ciberdelincuencia, la República del Perú se reserva el derecho a denegar la solicitud de conservación en virtud de dicho artículo en el caso que tenga motivos para creer que, en el momento de la revelación de los datos, no se cumplirá con la condición de la doble tipificación penal.

*MARTÍN VIZCARRA CORNEJO*
*Presidente de la República*

*CÉSAR VILLANUEVA ARÉVALO*
*Presidente del Consejo de Ministros*

*NÉSTOR POPOLIZIO BARDALES*
*Ministro de Relaciones Exteriores*

Carpeta de perfeccionamiento del Convenio sobre la Ciberdelincuencia

1. Informe (DGT) N° 030-2017

2. Copia autenticada del Convenio sobre la Ciberdelincuencia en inglés y francés

3. Traducción del Convenio sobre la Ciberdelincuencia

4. Solicitud de Perfeccionamiento

5. Carta de Invitación al Perú del Consejo de Europa

6. Opinión del Ministerio de Justicia y Derechos Humanos

7. Acta de Reunión Multisectorial de coordinación sobre Adhesión del Perú al Convenio de Budapest sobre Ciberdelincuencia

8. Opinión del Ministerio de Relaciones Exteriores

    - Dirección de Ciencia y Tecnología
    - Oficina de Cooperación Judicial

# Resolución Suprema Nº 209-2017-RE

Lima, 27 de setiembre de 2017

**CONSIDERANDO:**

Que, el Convenio sobre la Ciberdelincuencia fue adoptado en Budapest el 23 de noviembre de 2001;

Que, es conveniente a los intereses del Perú la aprobación del citado Convenio;

De conformidad con lo dispuesto en los artículos 56° y 102° inciso 3 de la Constitución Política del Perú y el primer párrafo del artículo 2° de la Ley N° 26647, que disponen la aprobación legislativa de los tratados celebrados por el Estado peruano;

**SE RESUELVE:**

**Artículo 1°.-** Remítase al Congreso de la República la documentación relativa al Convenio sobre la Ciberdelincuencia, adoptado en Budapest el 23 de noviembre de 2001.

**Artículo 2°.-** La presente Resolución Suprema será refrendada por la señora Presidenta del Consejo de Ministros y el señor Ministro de Relaciones Exteriores.

Regístrese, comuníquese y publíquese.

PEDRO PABLO KUCZYNSKI GODARD
Presidente de la República

MERCEDES ARAOZ FERNÁNDEZ
Presidenta del Consejo de Ministros

Registrado en la Fecha
27 SEP 2017
RS No 209 /.RE

RICARDO LUNA MENDOZA
Ministro de Relaciones Exteriores

# INFORME (DGT) N° 030-2017

## I. SOLICITUD DE PERFECCIONAMIENTO:

1.- Con Memorándum (DCT) N° DCT0122/2017 del 12 de junio de 2017, la Dirección de Ciencia y Tecnología del Ministerio de Relaciones Exteriores solicitó a la Dirección General de Tratados el inicio del procedimiento de perfeccionamiento del *"Convenio sobre la Ciberdelincuencia"*, adoptado en Budapest el 23 de noviembre de 2001 (en adelante, el Convenio).

## II. ANTECEDENTES:

2.- La problemática de los delitos cometidos por medios electrónicos motivó que en febrero de 1997 se establezca en el seno del Consejo de Europa[1] el 'Comité de Expertos en la Delincuencia en el Ciberespacio', con el mandato de preparar un instrumento jurídicamente vinculante que aborde esta materia.

3.- Las reuniones de negociación en el referido Comité se iniciaron en abril de 1997 y se prolongaron hasta junio de 2001, cuando el texto del Convenio negociado fue sometido a consideración del Comité Europeo para los Problemas Criminales, que lo aprobó en su 50° sesión, siendo considerado, luego, por el Comité de Ministros del Consejo de Europa, que también lo aprobó en su 109° sesión realizada en Budapest el 23 de noviembre de 2001.

4.- Desde ese momento, el Convenio quedó adoptado y abierto a la firma de los Estados miembros del Consejo de Europa y de los Estados no miembros que hubiesen participado en su elaboración.

5.- El Convenio es el primer tratado sobre delitos cometidos a través de internet y otros sistemas informáticos, que establece herramientas de derecho penal sustantivo y procesal así como en el plano de la cooperación judicial internacional para proteger a la sociedad frente a la ciberdelincuencia. Ello parte del reconocimiento, entre otros factores, del componente internacional que tiene esta problemática y que puede representar una limitación de la acción estatal unitaria en la persecución de estos delitos.

6.- El Convenio entró en vigor a nivel internacional el 1 de julio de 2004 al cumplirse las condiciones estipuladas en el propio instrumento[2].

7.- A partir de su entrada en vigor, los Estados que no son miembros del Consejo de Europa y que no hayan participado en la elaboración del Convenio pueden adherirse al Convenio siempre que hayan recibido una invitación del Comité de Ministros del Consejo de Europa, la cual, a su vez, debe haber tenido el consentimiento unánime de los Estados contratantes del Convenio[3].

8.- Mediante comunicación del 20 de febrero de 2015, el Director del Consejo Jurídico y de Derecho Internacional Público del Consejo de Europa se dirigió a la entonces Embajadora del Perú en Francia, para comunicar que el Comité de Ministros, en la 1220°

---

[1] El Consejo de Europa es una organización internacional regional cuyo objetivo es la defensa y protección de la democracia, el Estado de Derecho y los derechos humanos, en particular los civiles y políticos. Fue establecida en mayo de 1949 con el Tratado de Londres. Actualmente tiene como miembros a casi la totalidad de Estados europeos, con excepción de Bielorrusia. Tiene su sede en Estrasburgo, Francia. y su órgano más activo es el Tribunal Europeo de Derechos Humanos. Para mayor información, puede consultarse el siguiente enlace a la página web oficial de la organización: http://www.coe.int/web/about-us/who-we-are.

[2] Véase *infra*, párr. 58 de este informe.

[3] Ibíd., párr. 60.

reunión de delegados de los Ministros realizada el 18 de febrero de 2015, había decidido invitar al Perú a adherirse al Convenio.

9.- La citada comunicación precisa también que conforme a un acuerdo de los delegados de los Ministros adoptado en abril de 2013, las invitaciones tienen una validez de cinco años, tras lo cual expiran. Ello determina que la invitación recibida por el Perú se mantenga vigente sólo hasta el 18 de febrero de 2020.

10.- Debe notarse que la comunicación refiere que a través de una carta del 8 de setiembre, el Perú solicitó al Comité de Ministros del Consejo de Europa se le considere para ser invitado a adherirse al Convenio.

11.- A la fecha, el Convenio tiene 55 Partes, conforme al siguiente detalle[4]:

- 43 Estados miembros del Consejo de Europa lo han firmado y ratificado, lo que representa casi la totalidad de miembros de dicha organización, con excepción de Irlanda, Rusia, San Marino y Suecia;
- 3 Estados no miembros del Consejo de Europa lo han firmado y ratificado al haber participado en su elaboración: Canadá, Japón y Estados Unidos de América; y,
- 9 Estados no miembros del Consejo de Europa se han adherido: Australia, Chile, República Dominicana, Israel, Mauricio, Panamá, Senegal, Sri Lanka y Tonga.

12.- De otro lado, adicionalmente al Perú, también Colombia, Paraguay, Ghana y Nigeria han recibido invitación del Comité de Ministros del Consejo de Europa para adherirse al Convenio[5].

13.- El Convenio se encuentra registrado en el Archivo Nacional de Tratados 'Embajador Juan Miguel Bákula Patiño' con el código M-1071.

14.- Es importante mencionar que el Convenio cuenta, a su vez, con un Protocolo Adicional relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos, el cual fue adoptado en Estrasburgo el 28 de enero de 2003, y se encuentra en vigor internacionalmente desde el 1 de marzo de 2006[6]. No obstante, debe señalarse que este Protocolo Adicional no es objeto de la solicitud de perfeccionamiento, por lo que no ha sido comprendido en el presente informe.

## III. OBJETO:

15.- El Convenio busca armonizar los tipos penales vinculados a la ciberdelincuencia, así como determinadas reglas procesales necesarias que faciliten la investigación y procesamiento de este tipo delitos así como de aquellos cometidos mediante el uso de un sistema informático o los elementos probatorios que se encuentren en formato electrónico. Igualmente el Convenio busca definir algunas reglas que permitan disponer de un mecanismo rápido y eficaz de cooperación judicial internacional para contribuir a la persecución penal de este tipo de delitos.

## IV. DESCRIPCIÓN:

16.- El Convenio está conformado por un Preámbulo y un cuerpo principal de 48 artículos divididos en cuatro capítulos referidos a: Terminología, Medidas que deberán adoptarse a nivel nacional, Cooperación Internacional y Cláusulas Finales.

---

[4] Información obtenida de la página web del Consejo de Europa (http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185), consultada el 22 de agosto de 2017.

[5] Idem.

[6] Información obtenida de la página web del Consejo de Europa (http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189), consultada el 22 de agosto de 2017.

**Preámbulo**

17.- El Preámbulo, como parte integrante de los tratados, tiene una singular importancia, dado que en él se registran los motivos que llevaron a las Partes a negociar y, finalmente, a concluir un instrumento de esta naturaleza, lo que tiene relevancia a efectos de la interpretación de sus disposiciones.

18.- El Preámbulo del Convenio menciona que éste se gestó con la intención de aplicar una política penal común orientada a proteger a la sociedad frente a la ciberdelincuencia, en particular, mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional (párr. 4), como una respuesta articulada frente a los profundos cambios y retos que genera la digitalización, la convergencia y la globalización continuas de las redes informáticas (párr. 5).

19.- De esta forma, se deja entrever que el Convenio es concebido como necesario para prevenir acciones delictivas que puedan poner en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos (párr. 9), e incluso para reforzar la cooperación judicial internacional (párr. 8).

20.- Sin perjuicio de ello, se reconoce la necesidad de garantizar, por un lado, el debido equilibrio entre los intereses de la acción penal en la persecución y sanción de los delitos antes mencionados, y por el otro, el respeto de los derechos humanos fundamentales consagrados en tratados aplicables (párr. 10).

**Capítulo I - Terminología (artículo 1):**

21.- Este capítulo tiene como propósito establecer el sentido de una serie de expresiones, lo que contribuye a un entendimiento unívoco de los alcances de los compromisos contenidos en el Convenio.

22.- De esta manera, se definen las siguientes expresiones: 'sistema informático', 'datos informáticos', 'proveedor de servicios' y 'datos relativos al tráfico' (art. 1).

**Capítulo II - Medidas que deberán adoptarse a nivel nacional (artículos 2 al 22):**

23.- Este capítulo se subdivide en tres secciones referidas a derecho penal sustantivo (arts. 2 al 13), derecho procesal (arts. 14 al 21) y jurisdicción (art. 22).

24.- La **sección 1** sobre Derecho Penal sustantivo contempla el compromiso de los Estados para adoptar las medidas legislativas o de otro tipo que sean necesarias para tipificar una serie de tipos penales agrupados en 4 títulos, según se detalla a continuación:

a) En el Título 1, delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos: acceso ilícito (art. 2), interceptación ilícita (art. 3), ataques a la integridad de los datos (art. 4), ataques a la integridad del sistema (art. 5) y abuso de dispositivos (art. 6);

b) En el Título 2, delitos informáticos: falsificación informática (art. 7) y fraude informático (art. 8);

c) En el Título 3, delitos relacionados con el contenido: aquellos referidos a la pornografía infantil (art. 9); y,

d) En el título 4, delitos relacionados con infracciones de propiedad intelectual y de los derechos afines (art. 10).

25.- El Convenio exige también que las Partes adopten medidas legislativas o de otro tipo que sean necesarias para tipificar como delito la complicidad deliverada de los delitos anteriormente relacionados (art. 11.1) y, en ciertos casos, la tentativa deliberada (art. 11.2).

REPÚBLICA DEL PERÚ - Dirección General de Tratados - Ministerio de Relaciones Exteriores

REPÚBLICA DEL PERÚ - Copia Fiel de la Dirección General de Tratados - Ministerio de Relaciones Exteriores - P.C.B.

REPÚBLICA DEL PERÚ - Dirección General de Tratados - J.R.C - Ministerio de Relaciones Exteriores

26.- Es importante mencionar que las Partes pueden presentar declaraciones[7] para acogerse a la facultad de exigir uno o varios elementos complementarios previstos en las disposiciones sobre los delitos de acceso ilícito (art. 2)[8], interceptación ilícita (art. 3)[9], abuso de dispositivos (art. 6.1.b)[10], falsificación informática (art. 7)[11] y los delitos relacionados con la pornografía infantil (art. 9.3)[12].

27.- En el similar sentido, las Partes pueden acogerse a las reservas[13] expresamente contempladas en las disposiciones referidas a los delitos sobre ataques a la integridad de los datos (art. 4.2)[14], abuso de dispositivos (art. 6.3)[15], delitos relacionados con la pornografía infantil (art. 9.4)[16], delitos relacionados con la propiedad intelectual (art. 10.3)[17] y tentativa deliberada (art. 11.3)[18].

28.- Más adelante, al desarrollar la opinión del Ministerio de Justicia y Derechos Humanos, se ha incluido las declaraciones y reservas que esa entidad gubernamental ha estimado pertinente que el Perú formule, las cuales deben ser presentadas por escrito al momento de depositar el instrumento de adhesión del Perú[19].

29.- Igualmente, en la sección en comentario se establece la obligación de adoptar medidas legislativas o de otra índole que sean necesarias para definir reglas vinculadas a la responsabilidad de las personas jurídicas (art. 12), así como aquellas que permitan que los delitos señalados anteriormente tengan sanciones efectivas, proporcionadas y disuasorias no solamente para las personas naturales sino también para las personas jurídicas (art. 13).

30.- La **sección 2**, referida al Derecho Procesal establece reglas que deben ser adoptadas por los Estados a través de medidas legislativas o de otra índole, y que están orientadas a establecer los poderes y procedimientos relacionados con la persecución de los delitos cubiertos por el Convenio (previstos en los artículos 2 al 11), incluyendo a los delitos que se sirvan de sistemas informáticos para su comisión y a la obtención de elementos probatorios de cualquier delito (art. 14).

31.- En esa línea, el Convenio establece la obligación de adoptar medidas legislativas o de otra índole que permitan a las autoridades competentes de los Estados ordenar o imponer la conservación rápida de datos electrónicos específicos, en particular cuando los datos sean susceptibles de pérdida o modificación (art. 16), que garanticen la

---

[7] Véase *infra*, párr. 64 de este informe.

[8] Respecto al acceso ilícito, las Partes pueden exigir que el delito se haya cometido infringiendo medidas de seguridad con la intención de obtener datos informáticos o con otra intención distinta, o en relación con un sistema informático que esté conectado a otro sistema informático

[9] Respecto a la interceptación ilícita, las Partes pueden exigir que el delito se haya cometido con intención delictiva o en relación con un sistema informático conectado a otro sistema informático

[10] Las Partes pueden exigir en su derecho interno, a propósito del abuso de dispositivos, la posesión de un número determinado de elementos, como dispositivos o contraseñas, códigos de acceso para que se considere que existe responsabilidad penal.

[11] En la falsificación informática, las Partes pueden exigir que existe una intención dolosa o delictiva para que se considere que existe responsabilidad penal.

[12] Respecto a los delitos vinculados con la pornografía infantil, las Partes pueden exigir un límite de edad inferior a 18 años para considerar a los menores de edad.

[13] Véase *infra*, párr. 64 de este informe.

[14] En relación con los ataques a la integridad de los datos, las Partes pueden reservarse el derecho a exigir que los actos que configuren el delito deban generar daños graves.

[15] En el caso del abuso de dispositivos, las partes pueden reservarse el derecho a no adoptar las medidas de tipificación del delito en la medida que ésta no afecte la venta, distribución o cualesquiera otra forma de puesta a disposición de elementos como contraseñas, códigos de acceso o datos informáticos.

[16] En los delitos relacionados con la pornografía infantil, las Partes pueden reservarse el derecho a no tipificar la adquisición, para sí o para otros, de pornografía infantil a través de un sistema informático, la posesión de pornografía infantil en un sistema informático o dispositivo de almacenamiento, y a no considerar como pornografía infantil los casos en que una persona que aparente ser menor y adopte un comportamiento sexual explícito o imágenes realistas que representen a un menor adoptando también un comportamiento sexual explícito.

[17] Respecto a las infracciones de la propiedad intelectual y de derechos afines, las Partes pueden reservarse el derecho de no imponer responsabilidad penal las infracciones en este ámbito siempre que no se vulneren las obligaciones internacionales que incumban a las Partes.

[18] Las Partes pueden reservarse el todo o en parte la obligación de tipificar como delito la tentativa deliberada de los actos ilícitos cubiertos por el Convenio.

[19] Véase *infra*, párr. 96 a 98 de este informe.

REPÚBLICA DEL PERÚ - Dirección General de Tratados - Ministerio de Relaciones Exteriores

REPÚBLICA DEL PERÚ - Dirección General de Tratados - J.R.C - Ministerio de Relaciones Exteriores

REPÚBLICA DEL PERÚ - Dirección General de Tratados - P.C.B. - Ministerio de Relaciones Exteriores

conservación rápida de datos relativos al tráfico y aseguren la revelación rápida a la autoridad competente del Estado, o a una persona designada por dicha autoridad, de un volumen suficiente de datos relativos al tráfico para que la Parte pueda identificar tanto a los proveedores de servicios como la vía por la que la comunicación se ha transmitido (art. 17).

32.- Igualmente, el Convenio establece la obligación de las Partes de adoptar medidas legislativas o de otra índole que permitan que las autoridades competentes puedan ordenar a personas y proveedores de servicios la presentación de datos informáticos (art. 18), registrar y confiscar datos informáticos almacenados (art. 19), obtener en tiempo real datos relativos al tráfico (art. 20) e interceptar datos informáticos relativos a un repertorio de delitos graves (art. 21).

33.- A propósito de la obtención en tiempo real de datos relativos al tráfico, es importante anotar que el Convenio permite que las Partes puedan formular una reserva sobre la aplicación de las medidas allí mencionadas (art. 14.3)[20].

34.- Un compromiso importante que asumen las Partes en virtud del Convenio es asegurar que en la ejecución del mismo, es decir, en el establecimiento, ejecución y aplicación de los procedimientos penales relacionados con los delitos previstos en él, se garantice una protección adecuada de los derechos humanos y de las libertades, tomándose como referencia, para tal efecto, los derechos y libertades que las Partes hayan asumido en virtud del Convenio del Consejo de Europa para la protección de los derechos humanos y las libertades fundamentales (1950), del Pacto Internacional de derechos civiles y políticos de las Naciones Unidas (1966), y de otros instrumentos internacionales aplicables en materia de derechos humanos, así como integrar el principio de proporcionalidad (art. 15, condiciones y salvaguardias).

35.- En cuanto a la **sección 3** sobre jurisdicción, debe destacarse que el Convenio no excluye ninguna jurisdicción penal ejercida por una Parte de conformidad con su derecho interno (art. 22.4). No obstante, establece la obligación de los Estados de adoptar las medidas legislativas o de otro tipo que sean necesarias para afirmar la jurisdicción del Estado respecto de cualquiera de los delitos previstos en el Convenio cuando éste se hubiera cometido en su territorio; a bordo de un buque que enarbole su pabellón; a bordo de una aeronave matriculada según sus leyes; o por uno de sus nacionales si el delito es susceptible de sanción penal en el lugar en el que se cometió si ningún Estado tiene competencia territorial (art. 22.1). Debe indicarse, no obstante, que el Convenio permite que las Partes puedan formular una reserva sobre los alcances de las disposiciones en comentario (art. 22.2)[21].

36.- El Convenio también establece el compromiso de adoptar medidas para afirmar la jurisdicción respecto de cualquier delito cubierto por la Convención cuando el presunto autor se encuentre en su territorio y no pueda ser extraditado a otra Parte por razón únicamente de su nacionalidad (art. 22.3). Además, se ha previsto que en caso varias Partes estimasen que tienen jurisdicción respecto de un presunto delito previsto en el Convenio, dichas Partes deberán celebrar consultas a fin de decidir qué jurisdicción es la más adecuada para entablar la acción penal (art. 22.5).

**Capítulo III - Cooperación internacional (artículos 23 al 35):**

37.- Este capítulo contiene disposiciones vinculadas con la extradición y asistencia judicial mutua entre las Partes en relación con los delitos cubiertos por el Convenio, y

---

[20] Las Partes pueden reservarse el derecho a aplicar las medidas vinculadas a la obtención en tiempo real de datos relativos al tráfico únicamente a los delitos o categorías de delitos que se especifiquen en la reserva, siempre que dicho repertorio de delitos sea más reducido que el de los delitos a los que dicha Parte aplica las medidas relacionadas con la interceptación de datos relativos al tráfico.

[21] Las Partes puedan reservarse el derecho a no aplicar, o a aplicar sólo en determinados casos o condiciones, la jurisdicción de estos a [illegible] que enarbole su pabellón; a bordo de una aeronave matriculada según sus leyes; o por uno de sus nacionales si el delito es susceptible de sanción penal en el lugar en el que se cometió si ningún Estado tiene competencia territorial.

se divide en dos secciones, la primera, referida a Principios Generales (arts. 23 a 28) y la segunda, a Disposiciones Específicas (arts. 29 a 35).

38.- En la **sección 1** se desarrollan los principios generales aplicables a la cooperación internacional, a la extradición, la asistencia mutua, información espontánea, confidencialidad y restricciones de uso.

39.- En cuanto a los principios generales sobre cooperación, el Convenio establece el deber de las Partes de cooperar entre sí en las investigaciones o procedimientos relativos a delitos relacionados con sistemas y datos informáticos o para obtener pruebas de los delitos en formato electrónico, tomando como referencia las disposiciones del capítulo III en comentario, otros instrumentos aplicables sobre cooperación internacional en materia penal, los acuerdos basados en la legislación uniforme o recíproca y de su propio derecho interno (art. 23).

40.- En cuanto a la **extradición**, el Convenio prevé que la aplicación de estas disposiciones se dará en relación con los delitos previstos en el Convenio siempre que sean pasibles de una pena privativa de libertad de al menos un año o con una pena más grave conforme a la legislación de las dos Partes implicadas, o una pena inferior en caso se haya establecido así en un tratado de extradición aplicable a las dos Partes (art. 24.1).

41.- En esa línea, se señala que el Convenio puede ser tomado como base legal para conceder la extradición si una Parte condiciona la extradición a la existencia de un tratado y reciba una demanda de extradición de una Parte con la que no tiene celebrado ninguno (art. 24.3). Por el contrario, si las Partes no considerasen la existencia de un tratado como exigencia para la extradición, deberán reconocer que los delitos descritos en el Convenio pueden dar lugar a extradición (art. 24.4).

42.- Asimismo, se establece que las Partes considerarán que los delitos descritos en el Convenio están incluidos entre los delitos que pueden dar lugar a extradición en todos los tratados de esta materia concluido entre o por las Partes, y a incluirlos entre los delitos que puedan dar lugar a extradición en todos los tratados de extradición a concluirse entre las Partes (art. 24.2).

43.- El Convenio estipula que la extradición se sujetará a las condiciones previstas en el derecho interno de la Parte requerida o en los tratados de extradición vigentes, lo que incluirá los motivos por los que la extradición pudiera ser denegada (art. 24.5).

44.- En el caso que se deniegue una extradición por razón de la nacionalidad de la persona reclamada o porque la Parte requerida se considere competente, a pedido de la Parte requirente, la Parte requerida deberá someter el asunto a sus autoridades competentes e informará de su conclusión a la Parte requirente (art. 24.6).

45.- Las Partes deben comunicar al Secretario General del Consejo de Europa, al momento de firmar, ratificar, adherirse o aceptar el Convenio, el nombre y la dirección de cada autoridad responsable del envío o de la recepción de las demandas de extradición y de detención provisional en ausencia de tratado (art. 24.7.a), quien mantiene actualizado un registro de las autoridades designadas por las Partes (art. 24.7.b).

46.- Respecto a la **asistencia mutua**, las Partes asumen la obligación de prestarse toda la ayuda mutua posible a propósito de las investigaciones o de los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o con el fin de obtener pruebas en formato electrónico de cualquier delito (art. 25.1). Dicha asistencia se sujetará a lo previsto en el derecho interno de la Parte requerida o en los tratados aplicables, incluyendo los motivos para su rechazo (art. 25.4).

47.- El Convenio señala que, en casos de urgencia, las Partes podrán formular las solicitudes de asistencia mutua o realizar las comunicaciones relativas a la misma, a

REPÚBLICA DEL PERÚ - Dirección General de Tratados - Ministerio de Relaciones Exteriores - L.I.C.

REPÚBLICA DEL PERÚ - Dirección General de Tratados - Ministerio de Relaciones Exteriores - J.R.C.

REPÚBLICA DEL PERÚ - Dirección General de Tratados - Ministerio de Relaciones Exteriores - P.C.B.



10

través de medios de comunicación rápidos -fax o correo electrónico-, siempre que estos ofrezcan niveles suficientes de seguridad y autenticación, lo cual será aceptado por la Parte requerida, que responderá por cualquiera de esos medios (art. 25.3).

48.- Si la Parte requerida sujeta la prestación de asistencia judicial a la existencia de la doble tipificación, este requisito se considerará satisfecho si el acto que constituye delito relacionado con la solicitud de asistencia, está tipificado como tal en su derecho interno, independientemente que esté considerado o no en la misma categoría o tenga otra denominación (art. 25.5).

49.- El Convenio prevé también la posibilidad que las Partes, conforme a su derecho interno, puedan comunicarse información obtenida de sus propias investigaciones si consideran que ella puede ayudar a otra Parte a iniciar o concluir investigaciones o procedimientos penales en relación con los delitos previstos en el Convenio, o cuando esta información pueda conducir a una solicitud de asistencia judicial (art. 26).

50.- El Convenio exige que al momento de firmarlo, ratificarlo, adherirse o aceptarlo, las Partes designen a sus autoridades centrales, quienes podrán dirigirse entre sí y se encargarán de enviar las solicitudes de asistencia mutua, responderlas, ejecutarlas o remitirlas a las autoridades competentes para su ejecución (art. 27.2.a.b.c). En base a ello, el Secretario General del Consejo de Europa mantiene actualizado un registro de autoridades de las Partes para estos efectos (art. 27.2.d).

51.- El Convenio puede servir de base legal para la asistencia judicial en caso no exista un tratado aplicable entre las Partes requerida y requirente ni un acuerdo basado en la legislación uniforme o reciprocidad (art. 27.1). A tal efecto, el Convenio señala algunas disposiciones que deben seguir las Partes en relación con las solicitudes de asistencia judicial, entre ellas, que su ejecución se realizará conforme al derecho interno de la Parte requirente a menos que ello sea incompatible con el derecho interno de la Parte requerida (art. 27.3), que la prestación de la asistencia pueda ser aplazada si ésta perjudica investigaciones o procedimientos en curso (art. 27.5); y que la Parte requirente pueda solicitar la confidencialidad del trámite (art. 27.8).

52.- Es importante notar que el Convenio permite a las autoridades judiciales de una Parte dirigirse a sus homólogas de otra Parte para presentar solicitudes de asistencia y cursarse comunicaciones relativas a las mismas solo en casos de urgencia, sin perjuicio de enviar simultáneamene tales comunicaciones a las autoridades centrales (art. 27.9.a). Estas comunicaciones pueden también ser formuladas a través de la Organización Internacional de Policía Criminal – Interpol (art. 27.9.b).

53.- No obstante, las Partes pueden informar al Secretario General del Consejo de Europa, a través de una declaración escrita al momento de la firma, ratificación, adhesión o aceptación del Convenio, que en aras de la eficacia, las solicitudes en los casos de urgencia deben dirigirse a su autoridad central (art. 27, párr. 9.e)[22].

54.- El Convenio contempla también reglas de confidencialidad y restricciones de uso de la información que deberán ser aplicadas en ausencia de tratado de asistencia mutua o acuerdo basado en legislación uniforme entre la Parte requerida y requirente (art. 28).

55.- El Convenio establece, además, previsiones específicas sobre algunas modalidades que puede adoptar la asistencia mutua, bajo la forma de medidas provisionales, como la conservación rápida de datos informáticos almacenados (art. 29) y la revelación rápida de datos conservados (art. 30), o vinculados a poderes de investigación, como el acceso a datos almacenados (art. 31), el acceso transfronterizo a datos almacenados con consentimiento o cuando sean accesibles al público (art. 32), la obtención en tiempo real de datos relativos al tráfico (art. 33), o la interceptación de datos relativos al contenido (art. 34).

[22] Véase *infra*, párrafos 86 a 90 de este informe.

56.- El Convenio determina que las Partes designen a puntos de contacto localizables las 24 horas del día, los siete días a la semana (red 24/7), a fin de garantizar una asistencia inmediata para las investigaciones relativas a delitos vinculados a sistemas y datos informáticos o para obtener las pruebas en formato electrónico de un delito, y comprende toda acción que facilite medidas relativas a asesoramiento técnico, conservación de datos, obtención de pruebas, suministro de información de carácter jurídico y localización de sospechosos (art. 35).

**Capítulo IV - Cláusulas finales (artículos 36 al 48):**

57.- Las cláusulas finales de un tratado girán en torno a su entrada en vigor, enmiendas, entre otros aspectos operativos y de administración.

58.- El Convenio está abierto a la firma únicamente para los Estados miembros del Consejo de Europa y para los Estados no miembros que hayan participado en su elaboración (art. 36.1), encontrándose sujeto a ratificación, aceptación o aprobación mediante el depósito del instrumento respectivo con el Secretario General del Consejo de Europa (art. 36.2). Se precisa, además, como condición para su entrada en vigor, el primer día del mes siguiente al cumplimiento de un plazo de 3 meses contado desde la fecha en que 5 Estados hayan expresado su consentimiento en obligarse, de los cuales 3, como mínimo, sean miembros del Consejo de Europa (art. 36.3), lo cual se cumplió el 1 de julio de 2004.

59.- Tras su entrada en vigor, el Convenio entrará en vigor para los Estados signatarios que depositen su respectivo instrumento el primer día del mes siguiente a la expiración del plazo de 3 meses contado desde el depósito (art. 36.4).

60.- El Convenio se encuentra también abierto a la adhesión de Estados no miembros del Consejo de Europa que no hayan participado en su elaboración, empero esta posibilidad se encuentra sujeta a una invitación del Comité de Ministros del Consejo, la misma que debe ser aceptada por consentimiento unánime de sus miembros (art. 37.1). En estos casos, el Convenio entrará en vigor para el Estado adherente el primer día siguiente a la expiración del plazo de 3 meses contado desde el depósito del instrumento de adhesión, también con el Secretario General del Consejo de Europa (art. 37.2).

61.- Asimismo, las Partes pueden, al momento de depositar el instrumento de ratificación, aprobación, aceptación o adhesión, designar el territorio o territorios en los que se aplicará el Convenio (art. 38.1), la cual puede ser posteriormente extendida (art. 38.2) o retirada (art. 38.3).

62.- Se ha previsto que tiene por objeto Convenio complementar otros tratados, bilaterales o multilaterales, que sean aplicables entre las Partes, señalando, entre ellos, tratados en el marco del Consejo de Europa referidos a extradición y asistencia judicial penal (art. 39.1). Asimismo, se establece que si las Partes han celebrado otros tratados relativos a las materias abordadas en el Convenio, podrán aplicar dichos tratados o regular sus relaciones en base a ellos, en lugar del Convenio, siempre que no sea de forma incompatible con éste (art. 39.2). En cualquier caso, se deja claro que nada de lo dispuesto en el Convenio afecta otros derechos, restricciones y responsabilidades de cada Parte (art. 39.3).

63.- En el caso de los Estados federales, el Convenio les permite la formulación de reserva respecto al cumplimiento del capítulo II referido a las medidas de derecho penal sustantivo y procesal (art. 41.1)[23], la misma que no podrá excluir o reducir de manera sustancial la obligación del capítulo II y, en todo caso, se dotará de medios amplios y efectivos para aplicar las medidas previstas (art. 41.2).

[23] Los Estados federales pueden reservarse el derecho a cumplir las obligaciones del capítulo II en la medida que sean compatibles con los principios fundamentales que rijan las relaciones entre el gobierno central y los estados que lo constituyen o entidades territoriales análogas, a condición de garantizar la cooperación internacional prevista en el capítulo III.

P.C.B.

64.- Tal como fue indicado anteriormente, el Convenio permite, al momento de la firma o del depósito de instrumentos de ratificación, aprobación, aceptación o adhesión, la formulación de una serie de declaraciones referidas a elementos complementarios previstos en los artículos 2, 3, 6.1.b), 7, 9.3 y 27.9.e) (art. 40). Igualmente, en la misma oportunidad se permite la formulación de reservas únicamente a los artículos 4.2,6.3, 9.4, 10.3, 11.3, 14.3, 22.2, 29.4 y 41.1, quedando prohibida su formulación respecto de otras disposiciones (art. 42). Las reservas pueden ser retiradas total o parcialmente por la Parte que las haya formulado, mediante notificación al Secretario General del Consejo de Europa (art. 43.1), quedando obligado a ello tan pronto como lo permitan las circunstancias (art. 43.2).

65.- En cuanto a las enmiendas, el Convenio establece un procedimiento para ello, que se inicia con la presentación de propuestas de cualquiera de las Partes, las que serán comunicadas por el Secretario General del Consejo de Europa a todos los Estados miembros del Consejo, a todos los Estados no miembros que hubiesen participado en su elaboración, a los Estados que se hubiesen adherido y a aquellos que hubiesen sido invitados a adherirse (art. 44.1). Las propuestas de enmienda presentadas serán comunicadas al Comité Europeo para Problemas Criminales, que emitirá opinión y la someterá al Comité de Ministros (art. 44.2), el cual, luego de su examen y consulta con los Estados no miembros, podrá adoptar la enmienda (art. 44.3).

66.- Una vez adoptadas las enmiendas conforme al aludido procedimiento, éstas serán sometidas a las Partes para su aceptación (art. 44.4) y entrarán en vigor 30 días después que todas ellas hayan manifestado su aceptación (art. 44.5).

67.- Respecto a la solución de controversias, se prevé que las Partes involucradas intentarán llegar a un acuerdo mediante la negociación o cualquier medio de solución pacífica de controversias, incluyendo la sumisión de la controversia al Comité Europeo para Problemas Criminales (art. 45.2). Asimismo, el Convenio establece la obligación de mantener informado al referido Comité sobre la interpretación y aplicación del mismo (art. 45.1).

68.- El Convenio contempla un esquema de consultas directas entre las Partes acerca de la utilización y aplicación efectiva del mismo, el intercambio de información sobre novedades jurídicas, políticas o técnicas en relación con las materias abordadas, así como el estudio de la posibilidad de ampliarlo o enmendarlo, lo que debe ser informado periodicamente al Comité Europeo para Problemas Criminales (art. 46).

69.- Se ha previsto que cualquiera de las Partes puede denunciar el Convenio (art. 47. 1), la cual surtirá efectos el primer día del mes siguiente a la expiración del plazo de 3 meses contado desde la recepción, por el Secretario General del Consejo de Europa, de la notificación en ese sentido (art. 47.2).

70.- El Convenio señala que el Secretario General del Consejo de Europa tendrá la responsabilidad de notificar a los Estados miembros del Consejo, a los Estados no miembros que hubiesen participado en la elaboración del Convenio, a los Estados adherentes y a los que han sido invitado a adherirse, cualquier acto, notificación o comunicación relativa al Convenio, entre ellas, la firma, el depósito de instrumentos, las fechas de entrada en vigor para las Partes, las declaraciones y reservas presentadas.

71.- El Convenio fue adoptado únicamente en los idiomas inglés y francés, en ejemplar único, cuyos textos originales se encuentran en poder del Consejo de Europa.

## V. CALIFICACIÓN:

72.- El Convenio reúne los elementos formales exigidos por el Derecho Internacional para ser considerado como tratado, vale decir, haber sido celebrado entre sujetos de Derecho Internacional, originar derechos y obligaciones jurídicas y tener como marco

13

regulador al Derecho internacional, de conformidad con el criterio establecido en la Convención de Viena sobre el Derecho de los Tratados de 1969.

73.- La caracterización descrita es importante destacarla, dado que sólo aquellos instrumentos internacionales identificados como tratados son sometidos a perfeccionamiento interno en el Derecho peruano.

## VI. OPINIONES:

74.- Para la elaboración del presente informe, se ha tomado en consideración las opiniones emitidas por el Ministerio de Relaciones Exteriores y el Ministerio de Justicia y Derechos Humanos, así como del Poder Judicial, el Ministerio Público, la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros, la Secretaría de Defensa Nacional del Ministerio de Defensa y la Policía Nacional del Perú, que fueron expresadas en una reunión multisectorial y están reflejadas en un acta suscrita en dicha oportunidad.

### Ministerio de Relaciones Exteriores

75.- Al momento de solicitar el inicio del procedimiento de perfeccionamiento del Convenio, la Dirección de Ciencia y Tecnología, a través del Memorándum (DCT) N° DCT00122/2017, señaló su opinión en el sentido que la adhesión del Perú resulta importante y necesaria dado que ayudará a prevenir los actos que pongan en peligro la confidencialidad, la integridad y disponibilidad de sistemas, redes y datos informáticos, así como el abuso, lo que garantiza la tipificación, como delito, de dichos actos, facilitando su detección, investigación y posterior sanción, estableciendo, además, medidas que permitirán una cooperación judicial internacional rápida y fiable.

76.- En el mismo sentido, se expresa que la adhesión del Perú permitirá la aplicación a programas técnicos y de capacitación sobre Ciberdelincuencia y temas afines.

77.- Por todo ello, dicha oficina señala que de concretarse prontamente la adhesión, el Perú será pionero en Latinoamérica en la lucha frontal contra la ciberdelincuencia, y con ello, se logrará que el Perú y su sistema judicial, pueda beneficiar a la ciudadanía a través de las herramientas previstas en el Convenio.

78.- De otro lado, la mencionada oficina manifestó que en el proceso de conversaciones internas con miras a la adhesión del Perú, se realizaron coordinaciones con el Ministerio de Justicia y Derechos Humanos, el Poder Judicial, el Ministerio Público, la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros, la Secretaría de Defensa Nacional del Ministerio de Defensa y la Policía Nacional del Perú, en calidad de entidades gubernamentales competentes en las materias abordadas en el Convenio.

79.- Se destacó que con dichas entidades se convino en la necesidad que el Perú formule declaraciones y reservas dentro de lo permitido por el Convenio, acompañándose el texto de las mismas, encargando al Ministerio de Justicia y Derechos Humanos, como entidad competente, la evaluación y visto bueno a las mismas[24]. Igualmente, se convino en que las conformidades a fin de concretar la adhesión del Perú consten en un acta suscrita por los representantes de las entidades mencionadas en ocasión de una reunión multisectorial realizada el 31 de marzo de 2017.

80.- Con Memorándum (DCT) N° DCT0162/2017 del 18 de agosto de 2017, la misma oficina manifestó, de conformidad con el nuevo Código Procesal Penal aprobado por Decreto Legislativo N° 957, que para los efectos del capítulo III sobre cooperación internacional, el Ministerio Público-Fiscalía de la Nación, a través de la Unidad de Cooperación Judicial Internacional y Extradiciones, ejerce el rol de Autoridad Central del Perú en la materia y, en ese sentido, será la autoridad a cargo de enviar o recibir las solicitudes de extradición o de detención provisional a los efectos del artículo 24.7, de

24 Véase infra, párr. 96 y 99 de este informe.

la asistencia judicial conforme a lo dispuesto en el artículo 27.2, y ser el punto de contacto de la red 24/7 en los términos del artículo 35.1.

81.- Mediante Memorándum (OCJ) N° OCJ0339/2017 del 10 de julio de 2017, la Oficina de Cooperación Judicial de la Oficina General de Asuntos Legales se pronunció sobre el Convenio, en especial sobre el capítulo III referido a cooperación internacional.

82.- Sobre este último capítulo, la referida oficina señaló que el Convenio regula los procedimientos de extradición y asistencia judicial mutua, aspectos de relevancia para la persecución de los delitos informáticos, dada la universalidad de los mismos. En esa perspectiva, en lo que respecta a la extradición, destacó el compromiso de considerar incluidos en los tratados de extradición en vigor entre las Partes los delitos previstos en el Convenio como delitos que pueden dar lugar a la extradición, asimismo, el compromiso de incluirlos en los futuros tratados de extradición, y que el Convenio puede ser tomando como fundamento jurídico para solicitar la extradición en caso no se cuente con ningún tratado de extradición específico.

83.- A propósito de ello, la referida oficina expone sucintamente que los tratados de extradición actualmente están orientados a regular el procedimiento de extradición sin especificar los delitos a los que podría aplicarse, bastando sólo acreditar la doble incriminación, mientras que los tratados multilaterales están orientados a combatir determinados tipo de delitos, de conformidad con el bien jurídico que en cada caso se desee proteger, como ocurre con las Convenciones de las Naciones Unidas contra la Corrupción y contra la Delincuencia Organizada Transnacional y con el propio Convenio materia del presente informe.

84.- Teniendo en cuenta dichos elementos, la citada oficina manifestó que el Convenio puede ser invocado como base para un requerimiento de extradición, complementando un tratado bilateral sobre la materia que delinee un procedimiento.

85.- En cambio, si no existiese un tratado entre las Partes, el Convenio puede ser invocado directamente a fin de sustentar el requerimiento de extradición, y cualquier aspecto no previsto en él, se regirá por la legislación de las Partes.

86.- En base a tales consideraciones, la referida oficina consideró que el Convenio aborda implícitamente asuntos de derechos humanos por las garantías y derechos fundamentales de las personas y las reglas para viabilizar su remisión compulsiva, y de soberanía por el ejercicio del *ius puniendi* estatal, en la medida que el Estado requirente cuenta con jurisdicción respecto a los delitos cometidos en su territorio.

87.- En cuanto a la obligación de tipificar una serie de delitos, la referida oficina indicó que en virtud a la Ley de Delitos Informáticos, Ley N° 30096 y su modificatoria, Ley N° 30171, la normativa interna resulta compatible con el Convenio.

88.- En cuanto a la necesidad de designar una autoridad responsable de coordinar el envío y recepción de requerimientos vinculados con la asistencia judicial mutua, la Oficina señaló que la Autoridad Central peruana respecto a la cooperación judicial internacional en materia penal es, de acuerdo con el artículo 512 del Código Procesal Penal, la Fiscalía de la Nación, que asume sus funciones a través de la Unidad de Cooperación Judicial Internacional y Extradiciones.

**Ministerio de Justicia y Derechos Humanos**

89.- Mediante Oficio N° 584-2017-JUS/DGPCP del 15 de marzo de 2017, la Dirección General de Política Criminal y Penitenciaria se pronunció sobre el capítulo III referido a cooperación judicial, las adecuaciones normativas para la implementación íntegra del Convenio, y brinda algunos criterios en torno a los compromisos que derivan de los artículos 12 y 15 referidos a la responsabilidad penal de personas jurídicas y a las condiciones y salvaguardias en materia de derechos humanos, respectivamente.

15

90.- Sobre el capítulo III, la referida dependencia manifiesta que el nuevo Código Procesal Penal, aprobado mediante Decreto Legislativo N° 957, establece en su artículo 512 que la Autoridad Central para asuntos de cooperación judicial internacional en materia penal es la Fiscalía de la Nación, y, en base a la evaluación efectuada por la Dirección General de Justicia y Cultos, afirma que no se requieren mayores cambios sustanciales (modificación ni derogación) de darse la adhesión al Convenio.

91.- De otro lado, en relación con el impacto del íntegro del Convenio en la legislación peruana, la referida dependencia señaló que no es necesaria la modificación o derogación de alguna ley, o la aprobación de medidas legislativas para la ejecución.

92.- En cuanto al alcance del compromiso referido a la responsabilidad de las personas jurídicas previsto en el artículo 12 del Convenio, la mencionada Dirección General expuso el marco legal vigente que permite la imposición de sanciones a las personas jurídicas.

93.- Sobre el compromiso de garantizar la protección adecuada de los derechos humanos y libertades prevista en el artículo 15, en el oficio se destaca que la configuración de los procesos penales (investigación, juzgamiento y sanción) en el Perú se inscribe en el Estado de derecho y sobre la base del respeto de una serie de garantías vinculadas con los derechos fundamentales y, por ende, tienen relevancia constitucional señalando, entre ellos, el derecho fundamental a la libertad con la excepciones previstas en la ley, la observancia del debido proceso, la presunción de inocencia, el principio *non bis in idem*, legitimidad de las pruebas y el principio a no ser privado de la defensa.

94.- En esa línea, se reconoce que tales garantías guardan estricta observancia de los principios y derechos fundamentales consagrados en la Constitución Política, así como en los instrumentos internacionales de los que el Perú es Parte, como la Declaración Universal de Derechos Humanos, la Declaración Americana de Derechos y Deberes del Hombre, el Pacto Internacional de Derechos Civiles y Políticos, la Convención Americana de Derechos Humanos, entre otros.

- 95.- Con el Informe N° 28-2017-JUS/DGJC-DCJI del 8 de marzo de 2017, la Dirección de Cooperación Judicial Internacional presentó una evaluación del capítulo III referido a cooperación internacional, cubriendo los compromisos que asumiría el Perú en materia de extradición y cooperación judicial, constatando que sus alcances no contravienen la normativa nacional.

- 96.- Mediante Informe Usuario N° 14-2017-JUS/DGAC del 18 de agosto de 2017, la Dirección General de Asuntos Criminológicos presentó la evaluación realizada sobre las declaraciones y reservas permitidas por el Convenio al amparo de lo previsto en los artículos 40 y 42.

97.- En la conclusiones del informe se presenta la posición del Ministerio de Justicia y Derechos Humanos, de manera fundamentada, acerca de conveniencia de que el Perú presente declaraciones conforme a los artículos 2, 3, 7, 9.3 y 27.9.e) y reservas en virtud de los artículos 6.3, 9.4 y 29.4 del Convenio, las cuales deben ser formalizadas al momento del depósito del instrumento de adhesión del Perú. En base a ello, se entiende que el referido Ministerio, tras la evaluación, no ha considerado pertinente la formulación de las demás declaraciones y reservas permitidas por el Convenio.

98.- Las declaraciones que el Ministerio de Justicia y Derechos Humanos ha propuesto que el Perú formule se presentan en el siguiente cuadro:

| Disposición del Convenio | Declaración propuesta por el Ministerio de Justicia y Derechos Humanos |
|---|---|
| **Art. 2, Acceso ilícito:** *"Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e* | De conformidad con lo dispuesto en el artículo 2 del Convenio sobre la Ciberdelincuencia, la República del Perú declara que su legislación exige que el delito |

| | |
|---|---|
| *ilegítimo a todo o parte de un sistema informático. Las Partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático".* | de acceso ilícito se cometa infringiendo medidas de seguridad. |
| **Art. 3, Interceptación ilícita:**<br><br>*"Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima por medios técnicos, de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos. Las Partes podrán exigir que el delito se cometa con intención delictiva o en relación con un sistema informático conectado a otro sistema informático".* | De conformidad con lo dispuesto en el artículo 3 del Convenio sobre la Ciberdelincuencia, la República del Perú declara que su legislación exige que el delito de interceptación ilícita se cometa con intención delictiva y que dicho delito puede cometerse en relación con un sistema informático conectado a otro sistema informático. |
| **Art. 7, Falsificación informática:**<br><br>*"Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente. Las Partes podrán exigir que exista una intención dolosa o delictiva similar para que se considere que existe responsabilidad penal".* | De conformidad con lo dispuesto en el artículo 7 del Convenio sobre la Ciberdelincuencia, la República del Perú declara que podrá exigir que exista una intención fraudulenta o delictiva similar, conforme a lo establecido en su derecho interno, para que las conductas descritas en dicho artículo generen responsabilidad penal. |
| **Art. 27, Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables:**<br><br>*"9. e) En el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, las Partes podrán informar al Secretario General del Consejo de Europa de que, en aras de la eficacia, las solicitudes formuladas en virtud del presente párrafo deberán dirigirse a su autoridad central".* | De conformidad con lo establecido en el artículo 27, numeral 9, literal e) del Convenio sobre la Ciberdelincuencia, la República del Perú declara que, en aras de la eficacia, las solicitudes efectuadas en virtud de lo dispuesto en el numeral 9 del Convenio deberán dirigirse a su autoridad central. |

99.- De otro lado, las reservas que el mismo ministerio propone que el Perú formule son las siguientes:

| Disposición del Convenio | Reserva propuesta por el Ministerio de Justicia y Derechos Humanos |
|---|---|
| **Art. 6, Abuso de los dispositivos:**<br><br>*"3. Las Partes podrán reservarse el derecho a no aplicar el párrafo 1 del presente artículo, siempre que dicha reserva no afecte a la venta, distribución o cualesquiera otras formas de puesta a disposición de los elementos mencionados en el inciso 1.a.ii) del presente artículo".* | De conformidad con lo dispuesto en el párrafo 3 del artículo 6 del Convenio sobre la Ciberdelincuencia, la República del Perú se reserva el derecho de no aplicar el artículo 6, párrafo 1, literal b del Convenio. |

REPÚBLICA DEL PERÚ - Dirección General de Tratados - Ministerio de Relaciones Exteriores - L.C.

REPÚBLICA DEL PERÚ - Dirección General de Tratados - Ministerio de Relaciones Exteriores - J.P.C.

REPÚBLICA DEL PERÚ - Dirección General de Tratados - Ministerio de Relaciones Exteriores - P.C.B.

| | |
|---|---|
| **Art. 9, Delitos relacionados con la pornografía infantil:**<br><br>*"4. Las Partes podrán reservarse el derecho a no aplicar, en todo o en parte, los apartados d) y e) del párrafo 1, y los apartados b) y c) del párrafo 2".* | De conformidad con el numeral 4 del artículo 9° del Convenio sobre la Ciberdelincuencia, la República del Perú considera que el bien jurídico tutelado en el derecho interno con respecto a la pornografía infantil es la libertad y/o indemnidad sexual de un menor, por lo que formula una reserva a los literales b) y c) del párrafo 2 del citado artículo, debido a que las conductas contempladas en dichas disposiciones no involucran la participación de un menor de edad. |
| **Art. 29, Conservación rápida de datos informáticos almacenados:**<br><br>*"4. Cuando una Parte exija la doble tipificación penal como condición para atender una solicitud de asistencia mutua con vistas al registro o al acceso por un medio similar, a la confiscación o a la obtención por un medio similar o a la revelación de datos almacenados en relación con delitos diferentes de los previstos de conformidad con los artículos 2 a 11 del presente Convenio, podrá reservarse el derecho a denegar la solicitud de conservación en virtud del presente artículo en caso de que tenga motivos para creer que, en el momento de la revelación de los datos, no se cumplirá la condición de doble tipificación penal".* | Conforme al numeral 4 del artículo 29 del Convenio sobre la Ciberdelincuencia, la República del Perú se reserva el derecho a denegar la solicitud de conservación en virtud de dicho artículo en el caso que tenga motivos para creer que, en el momento de la revelación de los datos, no se cumplirá con la condición de la doble tipificación penal. |

**Acta de reunión multisectorial**

100.- Tal como se indicó a propósito de lo señalado por la Dirección de Ciencia y Tecnología en el Memorándum (DCT) N° DCT0122/2017, el Ministerio de Relaciones Exteriores, el Ministerio de Justicia y Derechos Humanos, el Poder Judicial, el Ministerio Público, la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros, la Secretaría de Defensa Nacional del Ministerio de Defensa y la Policía Nacional del Perú acordaron en reunión realizada el 31 de marzo de 2017 la suscripción de un acta en la que se exponga su opinión sobre las ventajas y beneficios de la adhesión del Perú así como el análisis del impacto del Convenio en la legislación nacional.

101.- En la citada reunión, todas las entidades expresaron su conformidad con el Convenio y reiteraron su opinión favorable (punto 1), destacándolo como una herramienta que complementa la legislación nacional de los Estados, lo que ayuda a fortalecer los mecanismos de protección de la sociedad frente a la ciberdelincuencia (punto 2, primer párrafo).

102.- En esa línea, las entidades manifestaron que el Convenio es importante y necesario porque coadyuva a la prevención, la lucha efectiva y eficaz, y la cooperación en relación con los referidos delitos (punto 2, segundo párrafo), además por el beneficio de la cooperación entre las Partes del Convenio, lo que también fortalecerá las capacidades del Perú para combatir estos delitos (punto 2, tercer párrafo).

103.- En lo referido al impacto del Convenio en la legislación peruana, las entidades manifestaron que la legislación vigente incorpora los supuestos delictivos previstos en el Convenio, precisando que la Dirección General de Política Criminal como la Dirección General de Justicia y Cultos del Ministerio de Justicia y Derechos Humanos han señalado que los artículos del Convenio son acordes con la legislación nacional vigente (punto 3).

104.- Por ello, las entidades concluyeron en que el Convenio no requiere la derogación o modificación de leyes ni la emisión de medidas legislativas con rango de ley para su ejecución (punto 4).

REPUBLICA DEL PERU - Dirección General de Asuntos Económicos y Tratados - Ministerio de Relaciones Exteriores

REPUBLICA DEL PERU - Dirección General de Asuntos Económicos y Tratados - P.C.B. - Ministerio de Relaciones Exteriores

18

105.- De otro lado, las entidades consideraron pertinente que el Perú formule declaraciones y reservas conforme a lo previsto en los artículos 40 y 42 del Convenio, por lo que validaron la propuesta de redacción presentada y delegaron al Ministerio de Justicia y Derechos Humanos la evaluación y visto bueno final respecto a cada una de ellas (punto 5).

## VII. VÍA DE PERFECCIONAMIENTO:

106.- Luego del estudio y análisis del expediente con los informes sectoriales, la Dirección General de Tratados concluye que el Convenio se enmarca en los supuestos de derechos humanos y soberanía, previstos en los numerales 1 y 2, respectivamente, del artículo 56 de la Constitución Política del Perú.

107.- La vinculación con los derechos humanos parte del reconocimiento que se hace en el Preámbulo de la necesidad de garantizar el debido equilibrio entre los intereses de la acción penal, vinculado a la ciberdelincuencia, con el respeto de los derechos humanos consagrados a nivel internacional.

108.- En desarrollo de dicho reconocimiento, el artículo 15 del Convenio establece el deber que tienen todas las Partes del Convenio de *"garantizar una protección adecuada de los derechos humanos y de las libertades"* teniendo como marco de referencia tratados de derechos humanos, como el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas de 1966.

109.- Es importante notar, como lo manifestado el Ministerio de Justicia y Derechos Humanos, que el nuevo Código Procesal Penal aprobado por Decreto Legislativo Nº 957 ha sido elaborado sobre la base del reconocimiento de las garantías y derechos fundamentales, tanto del imputado como del agraviado. Por citar algunos ejemplos, en los artículos 253 y 356 del Código, referidos a medidas de coerción procesal y juzgamiento, respectivamente, de forma explícita se reitera la aplicación de lo dispuesto en los tratados sobre derechos humanos aprobados y ratificados por el Perú.

110.- En la misma línea, tales garantías son aplicables también en la cooperación judicial en materia penal, debiendo anotar que el artículo 508 del mismo Código menciona, como parte de la normativa que rige las relaciones entre las autoridades nacionales con las extranjeras en esa materia, el marco de respecto de los derechos humanos.

111.- Esta relación puede ser apreciada más fácilmente si se tiene en cuenta que una persona privada de su libertad, en el marco de un proceso judicial en curso, se encuentra en una situación en la que sus derechos fundamentales más elementales pueden ser vulnerados, al igual que una persona reclamada para ser extraditada por otro Estado, toda vez que de ser concedida la extradición, se formalizaría su remisión compulsiva a ese otro Estado para efectos de juzgamiento, siendo ello la razón de ser del deber de garantía de la protección de los derechos y libertades prevista en el Convenio.

112.- En ese orden de ideas, puede afirmarse que aun cuando el Convenio no constituya, en sí mismo, un tratado de derechos humanos ni desarrolle ningún derecho humano en específico, puede afirmarse que promueve la aplicación de compromisos vinculados a derechos humanos. Por ello, a juicio de la Dirección General de Tratados, el Convenio versa sobre derechos humanos, en los términos del inciso 1 del artículo 56 de la Constitución Política.

113.- El supuesto de soberanía, por su parte, está dado por el hecho que el Convenio puede constituirse en la base legal para iniciar un procedimiento de extradición o concederse asistencia mutua, lo cual tiene que ver con el *ius puniendi*, potestad soberana para hacer efectivo el derecho penal del Estado, el cual se encuentra acotado

REPÚBLICA DEL PERÚ · Dirección General de Tratados · Ministerio de Relaciones Exteriores · R.C.

REPÚBLICA DEL PERÚ · Dirección General de Tratados · Ministerio de Relaciones Exteriores · J.R.C.

REPÚBLICA DEL PERÚ · Ministerio de Relaciones Exteriores · Dirección General de Tratados · P.C.B.

19

al territorio de cada Estado y debido al carácter transfronterizo de la ciberdelincuencia, ello constituye un hecho que limita al ejercicio de la referida potestad.

114.- De esta forma, en el caso de la extradición, el Convenio puede constituir una herramienta que permitirá el juzgamiento de personas procesadas o la ejecución de condenas en sus respectivos territorios, dado que materializará la entrega de la persona reclamada para los efectos antes señalados a través de la coordinación entre las autoridades competentes de las Partes. Igualmente, el Convenio facilitará la recíproca diligencia de actos judiciales fuera del territorio del Estado que lleva adelante el proceso.

115.- Por otro lado, no se aprecia que el Convenio contenga obligaciones internacionales vinculadas a dominio o integridad territorial, defensa nacional ni obligaciones financieras, tampoco crea, modifica o suprime tributos, ni exige la modificación o derogación de leyes ni requiere de medidas legislativas para su ejecución.

116.- A propósito de estos últimos supuestos, debe señalarse que de acuerdo al acta de reunión multisectorial del 31 de marzo de 2017, todas las entidades gubernamentales competentes en los asuntos abordados en el Convenio (Ministerio de Justicia y Derechos Humanos, Poder Judicial, Ministerio Público, Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros, Secretaría de Defensa Nacional del Ministerio de Defensa y Policía Nacional del Perú) expresaron que la adhesión del Perú no requiere la derogación o modificación de leyes ni la emisión de medidas legislativas con rango de ley para su ejecución. Dicha posición ha sido expuesta en el informe del Ministerio de Justicia y Derechos Humanos[25].

117.- Por las consideraciones antes referidas, la Dirección General de Tratados concluye que la vía que corresponde para el perfeccionamiento interno del Convenio es la dispuesta en el artículo 56 de la Constitución Política del Perú, que es desarrollada en el primer párrafo del artículo 2 de la Ley N° 26647 'Establecen normas que regulan los actos relativos al perfeccionamiento nacional de los tratados celebrados por el Estado peruano'.

118.- En consecuencia, corresponde que el Convenio sea, en primer término, aprobado por el Congreso de la República mediante resolución legislativa y luego ratificado internamente por el Presidente de la República mediante decreto supremo.

Lima, 23 de agosto de 2017.

REPÚBLICA DEL PERÚ - Dirección General de Tratados - Ministerio de Relaciones Exteriores

Jorge A. Raffo Carbajal
Embajador
Director General de Tratados
Ministerio de Relaciones Exteriores

REPÚBLICA DEL PERÚ - Dirección General de Tratados

REPÚBLICA DEL PERÚ - Fedatario de la Dirección General de Tratados - Ministerio de Relaciones Exteriores

[25] Véase supra, párr. 91 de este informe.

20

000018



# CONVENTION ON CYBERCRIME

# CONVENTION SUR LA CYBERCRIMINALITÉ

**Budapest, 23.XI.2001**

*European Treaty Series*
*Série des traités européens* / 185

**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





22

**Préambule**

Les Etats membres du Conseil de l'Europe et les autres Etats signataires,

Considérant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses membres ;

Reconnaissant l'intérêt d'intensifier la coopération avec les autres Etats parties à la Convention ;

Convaincus de la nécessité de mener, en priorité, une politique pénale commune destinée à protéger la société de la criminalité dans le cyberespace, notamment par l'adoption d'une législation appropriée et par l'amélioration de la coopération internationale ;

Conscients des profonds changements engendrés par la numérisation, la convergence et la mondialisation permanente des réseaux informatiques ;

Préoccupés par le risque que les réseaux informatiques et l'information électronique soient utilisés également pour commettre des infractions pénales et que les preuves de ces infractions soient stockées et transmises par le biais de ces réseaux ;

Reconnaissant la nécessité d'une coopération entre les Etats et l'industrie privée dans la lutte contre la cybercriminalité, et le besoin de protéger les intérêts légitimes dans l'utilisation et le développement des technologies de l'information ;

Estimant qu'une lutte bien menée contre la cybercriminalité requiert une coopération internationale en matière pénale accrue, rapide et efficace ;

Convaincus que la présente Convention est nécessaire pour prévenir les actes portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des systèmes informatiques, des réseaux et des données, ainsi que l'usage frauduleux de tels systèmes, réseaux et données, en assurant l'incrimination de ces comportements, tels que décrits dans la présente Convention, et l'adoption de pouvoirs suffisants pour permettre une lutte efficace contre ces infractions pénales, en en facilitant la détection, l'investigation et la poursuite, tant au plan national qu'au niveau international, et en prévoyant des dispositions matérielles en vue d'une coopération internationale rapide et fiable ;

Gardant à l'esprit la nécessité de garantir un équilibre adéquat entre les intérêts de l'action répressive et le respect des droits de l'homme fondamentaux, tels que garantis dans la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe (1950), dans le Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ainsi que dans d'autres conventions internationales applicables en matière de

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;

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;





24

droits de l'homme, qui réaffirment le droit à ne pas être inquiété pour ses opinions, le droit à la liberté d'expression, y compris la liberté de rechercher, d'obtenir et de communiquer des informations et des idées de toute nature, sans considération de frontière, ainsi que le droit au respect de la vie privée ;

Conscients également du droit à la protection des données personnelles, tel que spécifié, par exemple, par la Convention de 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Considérant la Convention des Nations Unies relative aux droits de l'enfant (1989) et la Convention de l'Organisation internationale du travail sur les pires formes de travail des enfants (1999) ;

Tenant compte des conventions existantes du Conseil de l'Europe sur la coopération en matière pénale, ainsi que d'autres traités similaires conclus entre les Etats membres du Conseil de l'Europe et d'autres Etats, et soulignant que la présente Convention a pour but de les compléter en vue de rendre plus efficaces les enquêtes et les procédures pénales portant sur des infractions pénales en relation avec des systèmes et des données informatiques, ainsi que de permettre la collecte des preuves électroniques d'une infraction pénale ;

Se félicitant des récentes initiatives destinées à améliorer la compréhension et la coopération internationales aux fins de la lutte contre la criminalité dans le cyberespace, notamment des actions menées par les Nations Unies, l'OCDE, l'Union européenne et le G8 ;

Rappelant les Recommandations du Comité des Ministres n° R (85) 10 concernant l'application pratique de la Convention européenne d'entraide judiciaire en matière pénale relative aux commissions rogatoires pour la surveillance des télécommunications, n° R (88) 2 sur des mesures visant à combattre la piraterie dans le domaine du droit d'auteur et des droits voisins, n° R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, n° R (95) 4 sur la protection des données à caractère personnel dans le domaine des services de télécommunication, eu égard notamment aux services téléphoniques, et n° R (89) 9 sur la criminalité en relation avec l'ordinateur, qui indique aux législateurs nationaux des principes directeurs pour définir certaines infractions informatiques, ainsi que n° R (95) 13 relative aux problèmes de procédure pénale liés à la technologie de l'information ;

Eu égard à la Résolution n° 1, adoptée par les ministres européens de la Justice lors de leur 21e Conférence (Prague, 10 et 11 juin 1997), qui recommande au Comité des Ministres de soutenir les activités concernant la cybercriminalité menées par le Comité européen pour les problèmes criminels (CDPC) afin de rapprocher les législations pénales nationales et de permettre l'utilisation de moyens d'investigation efficaces en matière d'infractions informatiques, ainsi qu'à la Résolution n° 3, adoptée lors de la 23e Conférence des ministres européens de la Justice (Londres, 8 et 9 juin 2000), qui encourage les parties aux négociations à poursuivre leurs efforts afin de trouver des solutions permettant au plus grand nombre d'Etats d'être parties à la Convention et qui reconnaît la nécessité de disposer d'un mécanisme rapide et efficace de coopération internationale qui tienne dûment compte des exigences spécifiques de la lutte contre la cybercriminalité ;

Prenant également en compte le plan d'action adopté par les chefs d'Etat et de gouvernement du Conseil de l'Europe à l'occasion de leur 2e Sommet (Strasbourg, 10 et 11 octobre 1997) afin de trouver des réponses communes au développement des nouvelles technologies de l'information, fondées sur les normes et les valeurs du Conseil de l'Europe,

25

Have agreed as follows:

## 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.





26

Sont convenus de ce qui suit :

## Chapitre I – Terminologie

### Article 1 – Définitions

Aux fins de la présente Convention,

a l'expression « système informatique » désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données ;

b l'expression « données informatiques » désigne toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction ;

c l'expression « fournisseur de services » désigne :

i toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique, et

ii toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs.

d « données relatives au trafic » désigne toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent.

## Chapitre II – Mesures à prendre au niveau national

### Section 1 – Droit pénal matériel

*Titre 1 – Infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques*

### Article 2 – Accès illégal

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.

### Article 3 – Interception illégale

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.

27

**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, the 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.

*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





28

**Article 4 – Atteinte à l'intégrité des données**

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques.

2 Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux.

**Article 5 – Atteinte à l'intégrité du système**

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques.

**Article 6 – Abus de dispositifs**

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, lorsqu'elles sont commises intentionnellement et sans droit :

a la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition :

i d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus ;

ii d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique,

dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5 ; et

b la possession d'un élément visé aux paragraphes a.i ou ii ci-dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5. Une Partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée.

2 Le présent article ne saurait être interprété comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au paragraphe 1 du présent article n'ont pas pour but de commettre une infraction établie conformément aux articles 2 à 5 de la présente Convention, comme dans le cas d'essai autorisé ou de protection d'un système informatique.

3 Chaque Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 du présent article, à condition que cette réserve ne porte pas sur la vente, la distribution ou toute autre mise à disposition des éléments mentionnés au paragraphe 1.a.ii du présent article.

*Titre 2 – Infractions informatiques*

**Article 7 – Falsification informatique**

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement

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;

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.





30

ou la suppression intentionnels et sans droit de données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles. Une Partie peut exiger une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée.

**Article 8 – Fraude informatique**

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui :

a par toute introduction, altération, effacement ou suppression de données informatiques ;

b par toute forme d'atteinte au fonctionnement d'un système informatique,

dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui.

*Titre 3 – Infractions se rapportant au contenu*

**Article 9 – Infractions se rapportant à la pornographie enfantine**

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les comportements suivants lorsqu'ils sont commis intentionnellement et sans droit :

a la production de pornographie enfantine en vue de sa diffusion par le biais d'un système informatique ;

b l'offre ou la mise à disposition de pornographie enfantine par le biais d'un système informatique ;

c la diffusion ou la transmission de pornographie enfantine par le biais d'un système informatique ;

d le fait de se procurer ou de procurer à autrui de la pornographie enfantine par le biais d'un système informatique ;

e la possession de pornographie enfantine dans un système informatique ou un moyen de stockage de données informatiques.

2 Aux fins du paragraphe 1 ci-dessus, le terme « pornographie enfantine » comprend toute matière pornographique représentant de manière visuelle :

a un mineur se livrant à un comportement sexuellement explicite ;

b une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite ;

c des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite.

3 Aux fins du paragraphe 2 ci-dessus, le terme « mineur » désigne toute personne âgée de moins de 18 ans. Une Partie peut toutefois exiger une limite d'âge inférieure, qui doit être au minimum de 16 ans.

4 Une Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, les paragraphes 1, alinéas d. et e, et 2, alinéas b. et c.

31

*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.

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



32

*Titre 4 – Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes*

**Article 10 – Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes**

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes à la propriété intellectuelle, définies par la législation de ladite Partie, conformément aux obligations que celle-ci a souscrites en application de l'Acte de Paris du 24 juillet 1971 portant révision de la Convention de Berne pour la protection des œuvres littéraires et artistiques, de l'Accord sur les aspects commerciaux des droits de propriété intellectuelle et du traité de l'OMPI sur la propriété intellectuelle, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.

2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes aux droits connexes définis par la législation de ladite Partie, conformément aux obligations que cette dernière a souscrites en application de la Convention internationale pour la protection des artistes interprètes ou exécutants, des producteurs de phonogrammes et des organismes de radiodiffusion (Convention de Rome), de l'Accord relatif aux aspects commerciaux des droits de propriété intellectuelle et du Traité de l'OMPI sur les interprétations et exécutions, et les phonogrammes, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.

3 Une Partie peut, dans des circonstances bien délimitées, se réserver le droit de ne pas imposer de responsabilité pénale au titre des paragraphes 1 et 2 du présent article, à condition que d'autres recours efficaces soient disponibles et qu'une telle réserve ne porte pas atteinte aux obligations internationales incombant à cette Partie en application des instruments internationaux mentionnés aux paragraphes 1 et 2 du présent article.

*Titre 5 – Autres formes de responsabilité et de sanctions*

**Article 11 – Tentative et complicité**

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute complicité lorsqu'elle est commise intentionnellement en vue de la perpétration d'une des infractions établies en application des articles 2 à 10 de la présente Convention, dans l'intention qu'une telle infraction soit commise.

2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute tentative intentionnelle de commettre l'une des infractions établies en application des articles 3 à 5, 7, 8, 9.1.a et c de la présente Convention.

3 Chaque Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 2 du présent article.

**Article 12 – Responsabilité des personnes morales**

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les personnes morales puissent être tenues pour responsables des infractions établies en application

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:

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.



34

de la présente Convention, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, fondé :

a sur un pouvoir de représentation de la personne morale ;

b sur une autorité pour prendre des décisions au nom de la personne morale ;

c sur une autorité pour exercer un contrôle au sein de la personne morale.

2 Outre les cas déjà prévus au paragraphe 1 du présent article, chaque Partie adopte les mesures qui se révèlent nécessaires pour s'assurer qu'une personne morale peut être tenue pour responsable lorsque l'absence de surveillance ou de contrôle de la part d'une personne physique mentionnée au paragraphe 1 a rendu possible la commission des infractions établies en application de la présence Convention pour le compte de ladite personne morale par une personne physique agissant sous son autorité.

3 Selon les principes juridiques de la Partie, la responsabilité d'une personne morale peut être pénale, civile ou administrative.

4 Cette responsabilité est établie sans préjudice de la responsabilité pénale des personnes physiques ayant commis l'infraction.

**Article 13 – Sanctions et mesures**

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les infractions pénales établies en application des articles 2 à 11 soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté.

2 Chaque Partie veille à ce que les personnes morales tenues pour responsables en application de l'article 12 fassent l'objet de sanctions ou de mesures pénales ou non pénales effectives, proportionnées et dissuasives, comprenant des sanctions pécuniaires.

## Section 2 – Droit procédural

*Titre 1 – Dispositions communes*

**Article 14 – Portée d'application des mesures du droit de procédure**

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour instaurer les pouvoirs et procédures prévus dans la présente section aux fins d'enquêtes ou de procédures pénales spécifiques.

2 Sauf disposition contraire figurant à l'article 21, chaque Partie applique les pouvoirs et procédures mentionnés dans le paragraphe 1 du présent article :

a aux infractions pénales établies conformément aux articles 2 à 11 de la présente Convention ;

b à toutes les autres infractions pénales commises au moyen d'un système informatique ; et

c à la collecte des preuves électroniques de toute infraction pénale.

3 a Chaque Partie peut se réserver le droit de n'appliquer les mesures mentionnées à l'article 20 qu'aux infractions ou catégories d'infractions spécifiées dans la réserve, pour autant que l'éventail de ces infractions ou catégories d'infractions ne soit pas plus réduit que celui des infractions auxquelles elle applique les mesures mentionnées à l'article 21. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée à l'article 20.

35

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.

*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.



36

b Lorsqu'une Partie, en raison des restrictions imposées par sa législation en vigueur au moment de l'adoption de la présente Convention, n'est pas en mesure d'appliquer les mesures visées aux articles 20 et 21 aux communications transmises dans un système informatique d'un fournisseur de services:

i qui est mis en œuvre pour le bénéfice d'un groupe d'utilisateurs fermé, et

ii qui n'emploie pas les réseaux publics de télécommunication et qui n'est pas connecté à un autre système informatique, qu'il soit public ou privé,

cette Partie peut réserver le droit de ne pas appliquer ces mesures à de telles communications. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée aux articles 20 et 21.

**Article 15 – Conditions et sauvegardes**

1 Chaque Partie veille à ce que l'instauration, la mise en œuvre et l'application des pouvoirs et procédures prévus dans la présente section soient soumises aux conditions et sauvegardes prévues par son droit interne, qui doit assurer une protection adéquate des droits de l'homme et des libertés, en particulier des droits établis conformément aux obligations que celle-ci a souscrites en application de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe (1950) et du Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ou d'autres instruments internationaux applicables concernant les droits de l'homme, et qui doit intégrer le principe de la proportionnalité.

2 Lorsque cela est approprié, eu égard à la nature de la procédure ou du pouvoir concerné, ces conditions et sauvegardes incluent, entre autres, une supervision judiciaire ou d'autres formes de supervision indépendante, des motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question.

3 Dans la mesure où cela est conforme à l'intérêt public, en particulier à la bonne administration de la justice, chaque Partie examine l'effet des pouvoirs et procédures dans cette section sur les droits, responsabilités et intérêts légitimes des tiers.

*Titre 2 – Conservation rapide de données informatiques stockées*

**Article 16 – Conservation rapide de données informatiques stockées**

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.

2 Lorsqu'une Partie fait application du paragraphe 1 ci-dessus, au moyen d'une injonction ordonnant à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, cette Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée aussi longue que nécessaire, au maximum de quatre-vingt-dix jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction soit renouvelée par la suite.

37

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

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 by which can be established:

a the type of communication service used, the technical provisions taken thereto and the period of service;

b 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;

c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.



38

3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger le gardien des données ou une autre personne chargée de conserver celles-ci à garder le secret sur la mise en œuvre desdites procédures pendant la durée prévue par son droit interne.

4 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

**Article 17 – Conservation et divulgation partielle rapides de données relatives au trafic**

1 Afin d'assurer la conservation des données relatives au trafic, en application de l'article 16, chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires :

a pour veiller à la conservation rapide de ces données relatives au trafic, qu'un seul ou plusieurs fournisseurs de services aient participé à la transmission de cette communication ; et

b pour assurer la divulgation rapide à l'autorité compétente de la Partie, ou à une personne désignée par cette autorité, d'une quantité suffisante de données relatives au trafic pour permettre l'identification par la Partie des fournisseurs de services et de la voie par laquelle la communication a été transmise.

2 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

*Titre 3 – Injonction de produire*

**Article 18 – Injonction de produire**

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner :

a à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ou un support de stockage informatique ; et

b à un fournisseur de services offrant des prestations sur le territoire de la Partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.

2 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

3 Aux fins du présent article, l'expression « données relatives aux abonnés » désigne toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir :

a le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service ;

b l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services ;

c toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services.

39

*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 a computer system or part of it and computer data stored therein; and

b 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:

a seize or similarly secure a computer system or part of it or a computer-data storage medium;

b make and retain a copy of those computer data;

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



40

*Titre 4 – Perquisition et saisie de données informatiques stockées*

**Article 19 – Perquisition et saisie de données informatiques stockées**

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire :

a à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées ; et

b à un support du stockage informatique permettant de stocker des données informatiques sur son territoire.

2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1.a, et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou l'accès d'une façon similaire à l'autre système.

3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire les données informatiques pour lesquelles l'accès a été réalisé en application des paragraphes 1 ou 2. Ces mesures incluent les prérogatives suivantes :

a saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci, ou un support de stockage informatique ;

b réaliser et conserver une copie de ces données informatiques ;

c préserver l'intégrité des données informatiques stockées pertinentes ;

d rendre inaccessibles ou enlever ces données informatiques du système informatique consulté.

4 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visées par les paragraphes 1 et 2.

5 Les pouvoirs et procédures mentionnés dans cet article doivent être soumis aux articles 14 et 15.

*Titre 5 – Collecte en temps réel de données informatiques*

**Article 20 – Collecte en temps réel des données relatives au trafic**

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes :

a à collecter ou enregistrer par l'application de moyens techniques existant sur son territoire, et

41

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:

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.



42

b à obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes :

i à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou

ii à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer,

en temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique.

2 Lorsqu'une Partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1.a, elle peut à la place, adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au trafic associées à des communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.

3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté ainsi que toute information à ce sujet.

4 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

**Article 21 – Interception de données relatives au contenu**

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes en ce qui concerne un éventail d'infractions graves à définir en droit interne :

a à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, et

b à obliger un fournisseur de services, dans le cadre de ses capacités techniques :

i à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou

ii à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer,

en temps réel, les données relatives au contenu de communications spécifiques sur son territoire, transmises au moyen d'un système informatique.

2 Lorsqu'une Partie, en raison des principes établis dans son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1.a, elle peut à la place adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au contenu de communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.

3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet.

4 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

43

### 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.

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.



44

### Section 3 – Compétence

#### Article 22 – Compétence

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction pénale établie conformément aux articles 2 à 11 de la présente Convention, lorsque l'infraction est commise :

a sur son territoire ; ou

b à bord d'un navire battant pavillon de cette Partie ; ou

c à bord d'un aéronef immatriculé selon les lois de cette Partie ; ou

d par un de ses ressortissants, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun Etat.

2 Chaque Partie peut se réserver le droit de ne pas appliquer, ou de n'appliquer que dans des cas ou des conditions spécifiques, les règles de compétence définies aux paragraphes 1.b à 1.d du présent article ou dans une partie quelconque de ces paragraphes.

3 Chaque Partie adopte les mesures qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction mentionnée à l'article 24, paragraphe 1, de la présente Convention, lorsque l'auteur présumé de l'infraction est présent sur son territoire et ne peut être extradé vers une autre Partie au seul titre de sa nationalité, après une demande d'extradition.

4 La présente Convention n'exclut aucune compétence pénale exercée par une Partie conformément à son droit interne.

5 Lorsque plusieurs Parties revendiquent une compétence à l'égard d'une infraction présumée visée dans la présente Convention, les Parties concernées se concertent, lorsque cela est opportun, afin de déterminer la mieux à même d'exercer les poursuites.

## Chapitre III – Coopération internationale

### Section 1 – Principes généraux

*Titre 1 – Principes généraux relatifs à la coopération internationale*

#### Article 23 – Principes généraux relatifs à la coopération internationale

Les Parties coopèrent les unes avec les autres, conformément aux dispositions du présent chapitre, en application des instruments internationaux pertinents sur la coopération internationale en matière pénale, des arrangements reposant sur des législations uniformes ou réciproques et de leur droit national, dans la mesure la plus large possible, aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et des données informatiques ou pour recueillir les preuves, sous forme électronique, d'une infraction pénale.

*Titre 2 – Principes relatifs à l'extradition*

#### Article 24 – Extradition

1 a Le présent article s'applique à l'extradition entre les Parties pour les infractions pénales définies conformément aux articles 2 à 11 de la présente Convention, à condition qu'elles soient punissables dans la législation des deux Parties concernées par une peine privative de liberté pour une période maximale d'au moins un an, ou par une peine plus sévère.

45

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.

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



46

b Lorsqu'il est exigé une peine minimale différente, sur la base d'un traité d'extradition tel qu'applicable entre deux ou plusieurs parties, y compris la Convention européenne d'extradition (STE n° 24), ou d'un arrangement reposant sur des législations uniformes ou réciproques, la peine minimale prévue par ce traité ou cet arrangement s'applique.

2 Les infractions pénales décrites au paragraphe 1 du présent article sont considérées comme incluses en tant qu'infractions pouvant donner lieu à extradition dans tout traité d'extradition existant entre ou parmi les Parties. Les Parties s'engagent à inclure de telles infractions comme infractions pouvant donner lieu à extradition dans tout traité d'extradition pouvant être conclu entre ou parmi elles.

3 Lorsqu'une Partie conditionne l'extradition à l'existence d'un traité et reçoit une demande d'extradition d'une autre Partie avec laquelle elle n'a pas conclu de traité d'extradition, elle peut considérer la présente Convention comme fondement juridique pour l'extradition au regard de toute infraction pénale mentionnée au paragraphe 1 du présent article.

4 Les Parties qui ne conditionnent pas l'extradition à l'existence d'un traité reconnaissent les infractions pénales mentionnées au paragraphe 1 du présent article comme des infractions pouvant donner lieu entre elles à l'extradition.

5 L'extradition est soumise aux conditions prévues par le droit interne de la Partie requise ou par les traités d'extradition en vigueur, y compris les motifs pour lesquels la Partie requise peut refuser l'extradition.

6 Si l'extradition pour une infraction pénale mentionnée au paragraphe 1 du présent article est refusée uniquement sur la base de la nationalité de la personne recherchée ou parce que la Partie requise s'estime compétente pour cette infraction, la Partie requise soumet l'affaire, à la demande de la Partie requérante, à ses autorités compétentes aux fins de poursuites, et rendra compte, en temps utile, de l'issue de l'affaire à la Partie requérante. Les autorités en question prendront leur décision et mèneront l'enquête et la procédure de la même manière que pour toute autre infraction de nature comparable, conformément à la législation de cette Partie.

7 a Chaque Partie communique au Secrétaire Général du Conseil de l'Europe, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, le nom et l'adresse de chaque autorité responsable de l'envoi ou de la réception d'une demande d'extradition ou d'arrestation provisoire, en l'absence de traité.

b Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités ainsi désignées par les Parties. Chaque Partie doit veiller en permanence à l'exactitude des données figurant dans le registre.

*Titre 3 – Principes généraux relatifs à l'entraide*

**Article 25 – Principes généraux relatifs à l'entraide**

1 Les Parties s'accordent l'entraide la plus large possible aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et à des données informatiques, ou afin de recueillir les preuves sous forme électronique d'une infraction pénale.

2 Chaque Partie adopte également les mesures législatives et autres qui se révèlent nécessaires pour s'acquitter des obligations énoncées aux articles 27 à 35.

3 Chaque Partie peut, en cas d'urgence, formuler une demande d'entraide ou les communications s'y rapportant par des moyens rapides de communication, tels que la télécopie ou le courrier

47

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.

### 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.





48

électronique, pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification (y compris, si nécessaire, le cryptage), avec confirmation officielle ultérieure si l'Etat requis l'exige. L'Etat requis accepte la demande et y répond par n'importe lequel de ces moyens rapides de communication.

4 Sauf disposition contraire expressément prévue dans les articles du présent chapitre, l'entraide est soumise aux conditions fixées par le droit interne de la Partie requise ou par les traités d'entraide applicables, y compris les motifs sur la base desquels la Partie requise peut refuser la coopération. La Partie requise ne doit pas exercer son droit de refuser l'entraide concernant les infractions visées aux articles 2 à 11 au seul motif que la demande porte sur une infraction qu'elle considère comme de nature fiscale.

5 Lorsque, conformément aux dispositions du présent chapitre, la Partie requise est autorisée à subordonner l'entraide à l'existence d'une double incrimination, cette condition sera considérée comme satisfaite si le comportement constituant l'infraction, pour laquelle l'entraide est requise, est qualifié d'infraction pénale par son droit interne, que le droit interne classe ou non l'infraction dans la même catégorie d'infractions ou qu'il la désigne ou non par la même terminologie que le droit de la Partie requérante.

**Article 26 – Information spontanée**

1 Une Partie peut, dans les limites de son droit interne et en l'absence de demande préalable, communiquer à une autre Partie des informations obtenues dans le cadre de ses propres enquêtes lorsqu'elle estime que cela pourrait aider la Partie destinataire à engager ou à mener à bien des enquêtes ou des procédures au sujet d'infractions pénales établies conformément à la présente Convention, ou lorsque ces informations pourraient aboutir à une demande de coopération formulée par cette Partie au titre du présent chapitre.

2 Avant de communiquer de telles informations, la Partie qui les fournit peut demander qu'elles restent confidentielles ou qu'elles ne soient utilisées qu'à certaines conditions. Si la Partie destinataire ne peut faire droit à cette demande, elle doit en informer l'autre Partie, qui devra alors déterminer si les informations en question devraient néanmoins être fournies. Si la Partie destinataire accepte les informations aux conditions prescrites, elle sera liée par ces dernières.

*Titre 4 – Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables*

**Article 27 – Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables**

1 En l'absence de traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, les dispositions des paragraphes 2 à 9 du présent article s'appliquent. Elles ne s'appliquent pas lorsqu'un traité, un arrangement ou une législation de ce type existent, à moins que les Parties concernées ne décident d'appliquer à la place tout ou partie du reste de cet article.

2 a Chaque Partie désigne une ou plusieurs autorités centrales chargées d'envoyer les demandes d'entraide ou d'y répondre, de les exécuter ou de les transmettre aux autorités compétentes pour leur exécution ;

49

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

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.



50

b Les autorités centrales communiquent directement les unes avec les autres ;

c Chaque Partie, au moment de la signature ou du dépôt de ses instruments de ratification, d'acceptation, d'approbation ou d'adhésion, communique au Secrétaire Général du Conseil de l'Europe les noms et adresses des autorités désignées en application du présent paragraphe ;

d Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités centrales désignées par les Parties. Chaque Partie veille en permanence à l'exactitude des données figurant dans le registre.

3 Les demandes d'entraide sous le présent article sont exécutées conformément à la procédure spécifiée par la Partie requérante, sauf lorsqu'elle est incompatible avec la législation de la Partie requise.

4 Outre les conditions ou les motifs de refus prévus à l'article 25, paragraphe 4, l'entraide peut être refusée par la Partie requise :

a si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique ; ou

b si la Partie requise estime que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels.

5 La Partie requise peut surseoir à l'exécution de la demande si cela risquerait de porter préjudice à des enquêtes ou procédures conduites par ses autorités.

6 Avant de refuser ou de différer sa coopération, la Partie requise examine, après avoir le cas échéant consulté la Partie requérante, s'il peut être fait droit à la demande partiellement, ou sous réserve des conditions qu'elle juge nécessaires.

7 La Partie requise informe rapidement la Partie requérante de la suite qu'elle entend donner à la demande d'entraide. Elle doit motiver son éventuel refus d'y faire droit ou l'éventuel ajournement de la demande. La Partie requise informe également la Partie requérante de tout motif rendant l'exécution de l'entraide impossible ou étant susceptible de la retarder de manière significative.

8 La Partie requérante peut demander que la Partie requise garde confidentiels le fait et l'objet de toute demande formulée au titre du présent chapitre, sauf dans la mesure nécessaire à l'exécution de ladite demande. Si la Partie requise ne peut faire droit à cette demande de confidentialité, elle doit en informer rapidement la Partie requérante, qui devra alors déterminer si la demande doit néanmoins être exécutée.

9 a En cas d'urgence, les autorités judiciaires de la Partie requérante peuvent adresser directement à leurs homologues de la Partie requise les demandes d'entraide ou les communications s'y rapportant. Dans un tel cas, copie est adressée simultanément aux autorités centrales de la Partie requise par le biais de l'autorité centrale de la Partie requérante.

b Toute demande ou communication formulée au titre du présent paragraphe peut l'être par l'intermédiaire de l'Organisation internationale de police criminelle (Interpol).

c Lorsqu'une demande a été formulée en application de l'alinéa a. du présent article et lorsque l'autorité n'est pas compétente pour la traiter, elle la transmet à l'autorité nationale compétente et en informe directement la Partie requérante.

d Les demandes ou communications effectuées en application du présent paragraphe qui ne supposent pas de mesure de coercition peuvent être directement transmises par les autorités compétentes de la Partie requérante aux autorités compétentes de la Partie requise.

51

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:

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;





52

e Chaque Partie peut informer le Secrétaire Général du Conseil de l'Europe, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, que, pour des raisons d'efficacité, les demandes faites sous ce paragraphe devront être adressées à son autorité centrale.

**Article 28 – Confidentialité et restriction d'utilisation**

1 En l'absence de traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, les dispositions du présent article s'appliquent. Elles ne s'appliquent pas lorsqu'un traité, un arrangement ou une législation de ce type existent, à moins que les Parties concernées ne décident d'appliquer à la place tout ou partie du présent article.

2 La Partie requise peut subordonner la communication d'informations ou de matériels en réponse à une demande :

a à la condition que ceux-ci restent confidentiels lorsque la demande d'entraide ne pourrait être respectée en l'absence de cette condition ; ou

b à la condition qu'ils ne soient pas utilisés aux fins d'enquêtes ou de procédures autres que celles indiquées dans la demande.

3 Si la Partie requérante ne peut satisfaire à l'une des conditions énoncées au paragraphe 2, elle en informe rapidement la Partie requise, qui détermine alors si l'information doit néanmoins être fournie. Si la Partie requérante accepte cette condition, elle sera liée par celle-ci.

4 Toute Partie qui fournit des informations ou du matériel soumis à l'une des conditions énoncées au paragraphe 2 peut exiger de l'autre Partie qu'elle lui communique des précisions, en relation avec cette condition, quant à l'usage fait de ces informations ou de ce matériel.

## Section 2 – Dispositions spécifiques

*Titre 1 – Entraide en matière de mesures provisoires*

**Article 29 – Conservation rapide de données informatiques stockées**

1 Une Partie peut demander à une autre Partie d'ordonner ou d'imposer d'une autre façon la conservation rapide de données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, et au sujet desquelles la Partie requérante a l'intention de soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation desdites données.

2 Une demande de conservation faite en application du paragraphe 1 doit préciser :

a l'autorité qui demande la conservation ;

b l'infraction faisant l'objet de l'enquête ou de procédures pénales et un bref exposé des faits qui s'y rattachent ;

c les données informatiques stockées à conserver et la nature de leur lien avec l'infraction ;

d toutes les informations disponibles permettant d'identifier le gardien des données informatiques stockées ou l'emplacement du système informatique ;

53

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.

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, or 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.



54

e la nécessité de la mesure de conservation ; et

f le fait que la Partie entend soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données informatiques stockées.

3 Après avoir reçu la demande d'une autre Partie, la Partie requise doit prendre toutes les mesures appropriées afin de procéder sans délai à la conservation des données spécifiées, conformément à son droit interne. Pour pouvoir répondre à une telle demande, la double incrimination n'est pas requise comme condition préalable à la conservation.

4 Une Partie qui exige la double incrimination comme condition pour répondre à une demande d'entraide visant la perquisition ou l'accès similaire, la saisie ou l'obtention par un moyen similaire ou la divulgation des données stockées peut, pour des infractions autres que celles établies conformément aux articles 2 à 11 de la présente Convention, se réserver le droit de refuser la demande de conservation au titre du présent article dans le cas où elle a des raisons de penser que, au moment de la divulgation, la condition de double incrimination ne pourra pas être remplie.

5 En outre, une demande de conservation peut être refusée uniquement :

a si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique ; ou

b si la Partie requise estime que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à l'ordre public ou à d'autres intérêts essentiels.

6 Lorsque la Partie requise estime que la conservation simple ne suffira pas à garantir la disponibilité future des données, ou compromettra la confidentialité de l'enquête de la Partie requérante, ou nuira d'une autre façon à celle-ci, elle en informe rapidement la Partie requérante, qui décide alors s'il convient néanmoins d'exécuter la demande.

7 Toute conservation effectuée en réponse à une demande visée au paragraphe 1 sera valable pour une période d'au moins soixante jours afin de permettre à la Partie requérante de soumettre une demande en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données. Après la réception d'une telle demande, les données doivent continuer à être conservées en attendant l'adoption d'une décision concernant la demande.

**Article 30 – Divulgation rapide de données conservées**

1 Lorsque, en exécutant une demande de conservation de données relatives au trafic concernant une communication spécifique formulée en application de l'article 29, la Partie requise découvre qu'un fournisseur de services dans un autre Etat a participé à la transmission de cette communication, la Partie requise divulgue rapidement à la Partie requérante une quantité suffisante de données concernant le trafic, aux fins d'identifier ce fournisseur de services et la voie par laquelle la communication a été transmise.

2 La divulgation de données relatives au trafic en application du paragraphe 1 peut être refusée seulement :

a si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique ; ou

b si elle considère que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels.

55

*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.

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

*Titre 2 – Entraide concernant les pouvoirs d'investigation*

**Article 31 – Entraide concernant l'accès aux données stockées**

1 Une Partie peut demander à une autre Partie de perquisitionner ou d'accéder de façon similaire, de saisir ou d'obtenir de façon similaire, de divulguer des données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, y compris les données conservées conformément à l'article 29.

2 La Partie requise satisfait à la demande en appliquant les instruments internationaux, les arrangements et les législations mentionnés à l'article 23, et en se conformant aux dispositions pertinentes du présent chapitre.

3 La demande doit être satisfaite aussi rapidement que possible dans les cas suivants :

a il y a des raisons de penser que les données pertinentes sont particulièrement sensibles aux risques de perte ou de modification ; ou

b les instruments, arrangements et législations visés au paragraphe 2 prévoient une coopération rapide.

**Article 32 – Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public**

Une Partie peut, sans l'autorisation d'une autre Partie :

a accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données ; ou

b accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre Etat, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique.

**Article 33 – Entraide dans la collecte en temps réel de données relatives au trafic**

1 Les Parties s'accordent l'entraide dans la collecte en temps réel de données relatives au trafic, associées à des communications spécifiées sur leur territoire, transmises au moyen d'un système informatique. Sous réserve des dispositions du paragraphe 2, cette entraide est régie par les conditions et les procédures prévues en droit interne.

2 Chaque Partie accorde cette entraide au moins à l'égard des infractions pénales pour lesquelles la collecte en temps réel de données concernant le trafic serait disponible dans une affaire analogue au niveau interne.

**Article 34 – Entraide en matière d'interception de données relatives au contenu**

Les Parties s'accordent l'entraide, dans la mesure permise par leurs traités et lois internes applicables, pour la collecte ou l'enregistrement en temps réel de données relatives au contenu de communications spécifiques transmises au moyen d'un système informatique.

*Titre 3 – Réseau 24/7*

**Article 35 – Réseau 24/7**

1 Chaque Partie désigne un point de contact joignable vingt-quatre heures sur vingt-quatre, sept jours sur sept, afin d'assurer une assistance immédiate pour des investigations concernant

57

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;

b the preservation of data pursuant to Articles 29 and 30;

c the collection of evidence, the provision of legal information, and locating of suspects.

2 a A Party's point of contact shall have the capacity to carry out communications 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.



58

les infractions pénales liées à des systèmes et à des données informatiques, ou pour recueillir les preuves sous forme électronique d'une infraction pénale. Cette assistance englobera la facilitation, ou, si le droit et la pratique internes le permettent, l'application directe des mesures suivantes :

a apport de conseils techniques ;

b conservation des données, conformément aux articles 29 et 30 ;

c recueil de preuves, apport d'informations à caractère juridique, et localisation des suspects.

2 a Le point de contact d'une Partie aura les moyens de correspondre avec le point de contact d'une autre Partie selon une procédure accélérée.

b Si le point de contact désigné par une Partie ne dépend pas de l'autorité ou des autorités de cette Partie responsables de l'entraide internationale ou de l'extradition, le point de contact veillera à pouvoir agir en coordination avec cette ou ces autorités, selon une procédure accélérée.

3 Chaque Partie fera en sorte de disposer d'un personnel formé et équipé en vue de faciliter le fonctionnement du réseau.

## Chapitre IV – Clauses finales

### Article 36 – Signature et entrée en vigueur

1 La présente Convention est ouverte à la signature des Etats membres du Conseil de l'Europe et des Etats non membres qui ont participé à son élaboration.

2 La présente Convention est soumise à ratification, acceptation ou approbation. Les instruments de ratification, d'acceptation ou d'approbation sont déposés près le Secrétaire Général du Conseil de l'Europe.

3 La présente Convention entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date à laquelle cinq Etats, incluant au moins trois Etats membres du Conseil de l'Europe, auront exprimé leur consentement à être liés par la Convention, conformément aux dispositions des paragraphes 1 et 2.

4 Pour tout Etat signataire qui exprimera ultérieurement son consentement à être lié par la Convention, celle-ci entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de l'expression de son consentement à être lié par la Convention, conformément aux dispositions des paragraphes 1 et 2.

### Article 37 – Adhésion à la Convention

1 Après l'entrée en vigueur de la présente Convention, le Comité des Ministres du Conseil de l'Europe peut, après avoir consulté les Etats contractants à la Convention et en avoir obtenu l'assentiment unanime, inviter tout Etat non membre du Conseil, n'ayant pas participé à son élaboration, à adhérer à la présente Convention. La décision est prise à la majorité prévue à l'article 20.d du Statut du Conseil de l'Europe et à l'unanimité des représentants des Etats contractants ayant le droit de siéger au Comité des Ministres.

2 Pour tout Etat adhérent à la Convention, conformément au paragraphe 1 ci-dessus, la Convention entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de dépôt de l'instrument d'adhésion près le Secrétaire Général du Conseil de l'Europe.

59

**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.

**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, 7, 9 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.



60

**Article 38 – Application territoriale**

1 Tout Etat peut, au moment de la signature ou au moment du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, désigner le ou les territoires auxquels s'appliquera la présente Convention.

2 Tout Etat peut, à tout autre moment par la suite, par déclaration adressée au Secrétaire Général du Conseil de l'Europe, étendre l'application de la présente Convention à tout autre territoire désigné dans la déclaration. La Convention entrera en vigueur à l'égard de ce territoire le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de la déclaration par le Secrétaire Général.

3 Toute déclaration faite en application des deux paragraphes précédents peut être retirée, en ce qui concerne tout territoire désigné dans cette déclaration, par notification adressée au Secrétaire Général du Conseil de l'Europe. Le retrait prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de ladite notification par le Secrétaire Général.

**Article 39 – Effets de la Convention**

1 L'objet de la présente Convention est de compléter les traités ou les accords multilatéraux ou bilatéraux applicables existant entre les Parties, y compris les dispositions :

- de la Convention européenne d'extradition, ouverte à la signature le 13 décembre 1957, à Paris (STE n° 24) ;
- de la Convention européenne d'entraide judiciaire en matière pénale, ouverte à la signature le 20 avril 1959, à Strasbourg (STE n° 30) ;
- du Protocole additionnel à la Convention européenne d'entraide judiciaire en matière pénale, ouvert à la signature le 17 mars 1978, à Strasbourg (STE n° 99).

2 Si deux ou plusieurs Parties ont déjà conclu un accord ou un traité relatif aux matières traitées par la présente Convention, ou si elles ont autrement établi leurs relations sur ces sujets, ou si elles le feront à l'avenir, elles ont aussi la faculté d'appliquer ledit accord ou traité ou d'établir leurs relations en conséquence, au lieu de la présente Convention. Toutefois, lorsque les Parties établiront leurs relations relatives aux matières faisant l'objet de la présente Convention d'une manière différente de celle y prévue, elles le feront d'une manière qui ne soit pas incompatible avec les objectifs et les principes de la Convention.

3 Rien dans la présente Convention n'affecte d'autres droits, restrictions, obligations et responsabilités d'une Partie.

**Article 40 – Déclarations**

Par déclaration écrite adressée au Secrétaire Général du Conseil de l'Europe, tout Etat peut, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, déclarer qu'il se prévaut de la faculté d'exiger, le cas échéant, un ou plusieurs éléments supplémentaires tels que prévus aux articles 2, 3, 6, paragraphe 1.b, 7, 9, paragraphe 3, et 27, paragraphe 9.e.

**Article 41 – Clause fédérale**

1 Un Etat fédéral peut se réserver le droit d'honorer les obligations contenues dans le chapitre II de la présente Convention dans la mesure où celles-ci sont compatibles avec les principes fondamentaux qui gouvernent les relations entre son gouvernement central et les Etats constituants ou autres entités territoriales analogues, à condition qu'il soit en mesure de coopérer sur la base du chapitre III.

61

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).

**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.



62

2 Lorsqu'il fait une réserve prévue au paragraphe 1, un Etat fédéral ne saurait faire usage des termes d'une telle réserve pour exclure ou diminuer de manière substantielle ses obligations en vertu du chapitre II. En tout état de cause, il se dote de moyens étendus et effectifs permettant la mise en oeuvre des mesures prévues par ledit chapitre.

3 En ce qui concerne les dispositions de cette Convention dont l'application relève de la compétence législative de chacun des Etats constituants ou autres entités territoriales analogues, qui ne sont pas, en vertu du système constitutionnel de la fédération, tenus de prendre des mesures législatives, le gouvernement fédéral porte, avec son avis favorable, lesdites dispositions à la connaissance des autorités compétentes des Etats constituants, en les encourageant à adopter les mesures appropriées pour les mettre en œuvre.

**Article 42 – Réserves**

Par notification écrite adressée au Secrétaire Général du Conseil de l'Europe, tout Etat peut, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, déclarer qu'il se prévaut de la ou les réserves prévues à l'article 4, paragraphe 2, à l'article 6, paragraphe 3, à l'article 9, paragraphe 4, à l'article 10, paragraphe 3, à l'article 11, paragraphe 3, à l'article 14, paragraphe 3, à l'article 22, paragraphe 2, à l'article 29, paragraphe 4, et à l'article 41, paragraphe 1. Aucune autre réserve ne peut être faite.

**Article 43 – Statut et retrait des réserves**

1 Une Partie qui a fait une réserve conformément à l'article 42 peut la retirer en totalité ou en partie par notification adressée au Secrétaire Général du Conseil de l'Europe. Ce retrait prend effet à la date de réception de ladite notification par le Secrétaire Général. Si la notification indique que le retrait d'une réserve doit prendre effet à une date précise, et si cette date est postérieure à celle à laquelle le Secrétaire Général reçoit la notification, le retrait prend effet à cette date ultérieure.

2 Une Partie qui a fait une réserve comme celles mentionnées à l'article 42 retire cette réserve, en totalité ou en partie, dès que les circonstances le permettent.

3 Le Secrétaire Général du Conseil de l'Europe peut périodiquement demander aux Parties ayant fait une ou plusieurs réserves comme celles mentionnées à l'article 42 des informations sur les perspectives de leur retrait.

**Article 44 – Amendements**

1 Des amendements à la présente Convention peuvent être proposés par chaque Partie, et sont communiqués par le Secrétaire Général du Conseil de l'Europe aux Etats membres du Conseil de l'Europe, aux Etats non membres ayant pris part à l'élaboration de la présente Convention, ainsi qu'à tout Etat y ayant adhéré ou ayant été invité à y adhérer, conformément aux dispositions de l'article 37.

2 Tout amendement proposé par une Partie est communiqué au Comité européen pour les problèmes criminels (CDPC), qui soumet au Comité des Ministres son avis sur ledit amendement.

3 Le Comité des Ministres examine l'amendement proposé et l'avis soumis par le CDPC et, après consultation avec les Etats non membres parties à la présente Convention, peut adopter l'amendement.

4 Le texte de tout amendement adopté par le Comité des Ministres conformément au paragraphe 3 du présent article est communiqué aux Parties pour acceptation.

5 Tout amendement adopté conformément au paragraphe 3 du présent article entre en vigueur le trentième jour après que toutes les Parties ont informé le Secrétaire Général de leur acceptation.

63

**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.

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.



64

**Article 45 – Règlement des différends**

1 Le Comité européen pour les problèmes criminels du Conseil de l'Europe (CDPC) est tenu informé de l'interprétation et de l'application de la présente Convention.

2 En cas de différend entre les Parties sur l'interprétation ou l'application de la présente Convention, les Parties s'efforceront de parvenir à un règlement du différend par la négociation ou par tout autre moyen pacifique de leur choix, y compris la soumission du différend au CDPC, à un tribunal arbitral qui prendra des décisions qui lieront les Parties au différend, ou à la Cour internationale de justice, selon un accord entre les Parties concernées.

**Article 46 – Concertation des Parties**

1 Les Parties se concertent périodiquement, au besoin, afin de faciliter :

a l'usage et la mise en œuvre effectifs de la présente Convention, y compris l'identification de tout problème en la matière, ainsi que les effets de toute déclaration ou réserve faite conformément à la présente Convention ;

b l'échange d'informations sur les nouveautés juridiques, politiques ou techniques importantes observées dans le domaine de la criminalité informatique et la collecte de preuves sous forme électronique ;

c l'examen de l'éventualité de compléter ou d'amender la Convention.

2 Le Comité européen pour les problèmes criminels (CDPC) est tenu périodiquement au courant du résultat des concertations mentionnées au paragraphe 1.

3 Le CDPC facilite, au besoin, les concertations mentionnées au paragraphe 1 et adopte les mesures nécessaires pour aider les Parties dans leurs efforts visant à compléter ou amender la Convention. Au plus tard à l'issue d'un délai de trois ans à compter de l'entrée en vigueur de la présente Convention, le CDPC procédera, en coopération avec les Parties, à un réexamen de l'ensemble des dispositions de la Convention et proposera, le cas échéant, les amendements appropriés.

4 Sauf lorsque le Conseil de l'Europe les prend en charge, les frais occasionnés par l'application des dispositions du paragraphe 1 sont supportés par les Parties, de la manière qu'elles déterminent.

5 Les Parties sont assistées par le Secrétariat du Conseil de l'Europe dans l'exercice de leurs fonctions découlant du présent article.

**Article 47 – Dénonciation**

1 Toute Partie peut, à tout moment, dénoncer la présente Convention par notification au Secrétaire Général du Conseil de l'Europe.

2 La dénonciation prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de la notification par le Secrétaire Général.

**Article 48 – Notification**

Le Secrétaire Général du Conseil de l'Europe notifie aux Etats membres du Conseil de l'Europe, aux Etats non membres ayant pris part à l'élaboration de la présente Convention, ainsi qu'à tout Etat y ayant adhéré ou ayant été invité à y adhérer :

a toute signature ;

b le dépôt de tout instrument de ratification, d'acceptation, d'approbation ou d'adhésion ;

c toute date d'entrée en vigueur de la présente Convention, conformément à ses articles 36 et 37 ;

d toute déclaration faite en application de l'article 40 ou toute réserve faite en application de l'article 42 ;

e tout autre acte, notification ou communication ayant trait à la présente Convention.

65

000063

CONSEIL DE L'EUROPE
COUNCIL OF EUROPE

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.

REPUBLICA DEL PERU
Dirección General de Tratados
L.A.M.P.
Ministerio de Relaciones Exteriores



66

CONSEIL DE L'EUROPE
COUNCIL OF EUROPE

En foi de quoi, les soussignés, dûment autorisés à cet effet, ont signé la présente Convention.

Fait à Budapest, le 23 novembre 2001, en français et en anglais, les deux textes faisant également foi, en un seul exemplaire qui sera déposé dans les archives du Conseil de l'Europe. Le Secrétaire Général du Conseil de l'Europe en communiquera copie certifiée conforme à chacun des Etats membres du Conseil de l'Europe, aux Etats non membres qui ont participé à l'élaboration de la Convention et à tout Etat invité à y adhérer.

**MINISTERIO DE RELACIONES EXTERIORES**
**DE LA REPÚBLICA DEL PERÚ**
**DIRECCIÓN GENERAL DE TRATADOS**

Se autentica el presente documento, que es

**"COPIA CERTIFICADA DEL INSTRUMENTO INTERNACIONAL"**

Que se conserva en el Archivo Nacional de Tratados "Embajador Juan Miguel Bákula Patiño", registrado con el código M-1071 y que consta de 47 páginas.

Lima, 22-08-2017

REPÚBLICA DEL PERÚ - Dirección General de Tratados - Ministerio de Relaciones Exteriores

Luis Armando Monteagudo Pacheco
Ministro Consejero
Subdirector de Registro y Archivo
Dirección General de Tratados
Ministerio de Relaciones Exteriores

67

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

*Serie de Tratados Europeos- n°185*

# CONVENIO SOBRE LA CIBERDELINCUENCIA

**Budapest, 23.XI.2001**

**Preámbulo**

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Han convenido en lo siguiente:

## Capítulo I – Terminología

### Artículo 1 – Definiciones

A los efectos del presente Convenio:

a. por "sistema informático" se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa;
b. por "datos informáticos" se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función;
c. por "proveedor de servicios" se entenderá:

   i. toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático, y
   ii. cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo;

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

## Capítulo II – Medidas que deberán adoptarse a nivel nacional

### Sección 1 – Derecho penal sustantivo

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

### Artículo 2 – Acceso ilícito

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

### Artículo 3 – Interceptación ilícita

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del

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

**Artículo 4 – Ataques a la integridad de los datos**

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

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

**Artículo 5 – Ataques a la integridad del sistema**

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

**Artículo 6 – Abuso de los dispositivos**

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

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

   i. cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de cualquiera de los delitos previstos en los artículos 2 a 5 del presente Convenio;
   ii. una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático,

   con intención de que sean utilizados para cometer cualquiera de los delitos contemplados en los artículos 2 a 5; y

b. la posesión de alguno de los elementos contemplados en los incisos i) o ii) del apartado a) del presente artículo con intención de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2 a 5. Las Partes podrán exigir en su derecho interno la posesión de un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

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

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

*Título 2 – delitos informáticos*

**Artículo 7 – Falsificación informática**

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

**Artículo 8 – Fraude informático**

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

a. la introducción, alteración, borrado o supresión de datos informáticos;
b. cualquier interferencia en el funcionamiento de un sistema informático,

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

*Título 3 – Delitos relacionados con el contenido*

**Artículo 9 – Delitos relacionados con la pornografía infantil**

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

a. la producción de pornografía infantil con la intención de difundirla a través de un sistema informático;
b. la oferta o la puesta a disposición de pornografía infantil a través de un sistema informático;
c. la difusión o la transmisión de pornografía infantil a través de un sistema informático;
d. la adquisición, para uno mismo o para otros, de pornografía infantil a través de un sistema informático;
e. la posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos.

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

a. un menor adoptando un comportamiento sexualmente explícito;
b. una persona que parezca un menor adoptando un comportamiento sexualmente explícito;
c. imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito.

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

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

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

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

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

2. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de los derechos afines definidas en su legislación, de conformidad con las obligaciones que haya asumido en aplicación de la Convención Internacional sobre la Protección de los Artistas Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas, a excepción de cualquier derecho moral conferido por dichos Convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

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

*Título 5 – Otras formas de responsabilidad y de sanción*

**Artículo 11 – Tentativa y complicidad**

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno cualquier complicidad deliberada con vistas a la comisión de alguno de los delitos previstos en aplicación de los artículos 2 a 10 del presente Convenio, con la intención de que dicho delito sea cometido.

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

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

**Artículo 12 – Responsabilidad de las personas jurídicas**

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que pueda exigirse responsabilidad a las personas jurídicas por los delitos previstos en aplicación del presente Convenio, cuando éstos sean cometidos por cuenta de las mismas por una persona física, ya sea a título individual o como miembro de un órgano de dicha persona jurídica, que ejerza funciones directivas en su seno, en virtud de:

a. un poder de representación de la persona jurídica;
b. una autorización para tomar decisiones en nombre de la persona jurídica;
c. una autorización para ejercer funciones de control en el seno de la persona jurídica.

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

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

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

**Artículo 13 – Sanciones y medidas**

1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para que los delitos previstos en aplicación de los artículos 2 a 11 estén sujetos a sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad.

2. Las Partes garantizarán la imposición de sanciones o medidas penales o no penales efectivas, proporcionadas y disuasorias, incluidas sanciones pecuniarias, a las personas jurídicas consideradas responsables de conformidad con el artículo 12.

**Sección 2 – Derecho procesal**

*Título 1 – Disposiciones comunes*

**Artículo 14 – Ámbito de aplicación de las disposiciones de procedimiento**

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

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

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

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

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

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

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

**Artículo 15 – Condiciones y salvaguardias**

1. Cada Parte se asegurará de que la instauración, ejecución y aplicación de los poderes y procedimientos previstos en la presente Sección se sometan a las condiciones y salvaguardias previstas en su derecho interno, que deberá garantizar una protección adecuada de los derechos humanos y de las libertades, y en particular de los derechos

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

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

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

*Título 2 – Conservación rápida de datos informáticos almacenados*

**Artículo 16 – Conservación rápida de datos informáticos almacenados**

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

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

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

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

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

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

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

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

*Título 3 – Orden de presentación*

**Artículo 18 – Orden de presentación**

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

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

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

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

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

*Título 4 – Registro y confiscación de datos informáticos almacenados*

**Artículo 19 – Registro y confiscación de datos informáticos almacenados**

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

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

en su territorio.

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

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

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

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

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

*Título 5 – Obtención en tiempo real de datos informáticos*

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

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

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

    i. a obtener o a grabar con medios técnicos existentes en su territorio, o

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

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

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

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

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

**Artículo 21 – Interceptación de datos relativos al contenido**

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

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

i. obtener o grabar con medios técnicos existentes en su territorio, o
ii. prestar a las autoridades competentes su colaboración y su asistencia para obtener o grabar,

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

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

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

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

**Sección 3 – Jurisdicción**

**Artículo 22 – Jurisdicción**

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

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

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

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

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

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

**Capítulo III – Cooperación internacional**

**Sección 1 – Principios generales**

*Título 1 – Principios generales relativos a la cooperación internacional*

**Artículo 23 – Principios generales relativos a la cooperación internacional**

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

*Título 2 – Principios relativos a la extradición*

**Artículo 24 – Extradición**

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

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

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

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

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

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

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

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

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

*Título 3 – Principios generales relativos a la asistencia mutua*

**Artículo 25 – Principios generales relativos a la asistencia mutua**

1. Las Partes se prestarán toda la ayuda mutua posible a efectos de las investigaciones o de los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o con el fin de obtener pruebas en formato electrónico de un delito.

2. Cada Parte adoptará asimismo las medidas legislativas y de otro tipo que resulten necesarias para cumplir con las obligaciones establecidas en los artículos 27 a 35.

3. Cada Parte podrá, en caso de urgencia, formular una solicitud de asistencia mutua, o realizar las comunicaciones relativas a la misma a través de medios de comunicación rápidos, como el fax o el correo electrónico, siempre que esos medios ofrezcan niveles suficientes de seguridad y de autenticación (incluido el criptado, en caso necesario), con confirmación oficial posterior si el Estado requerido así lo exige. El Estado requerido aceptará la solicitud y responderá a la misma por cualquiera de esos medios rápidos de comunicación.

4. Salvo en caso de que se disponga expresamente otra cosa en los artículos del presente Capítulo, la asistencia mutua estará sujeta a las condiciones establecidas en el derecho interno de la Parte requerida o en los tratados de asistencia mutua aplicables, incluidos los motivos sobre la base de los cuales la Parte requerida puede rechazar la cooperación. La Parte requerida no deberá ejercer su derecho a rehusar la asistencia mutua en relación con los delitos previstos en los artículos 2 a 11 únicamente porque la solicitud se refiera a un delito que dicha Parte considere de carácter fiscal.

5. Cuando, de conformidad con lo dispuesto en el presente Capítulo, la Parte requerida esté autorizada a condicionar la asistencia mutua a la existencia de doble tipificación penal, se considerará que dicha condición se satisface si el acto que constituye delito, y para el que se solicita la asistencia mutua, está tipificado como tal en su derecho interno, independientemente de que dicho derecho interno incluya o no el delito en la misma categoría o lo denomine o no con la misma terminología que la Parte requirente.

**Artículo 26 – Información espontánea**

1. Dentro de los límites de su derecho interno y sin que exista demanda previa, una Parte podrá comunicar a otra Parte información obtenida de sus propias investigaciones si considera que ello puede ayudar a la Parte destinataria a iniciar o a concluir investigaciones o procedimientos en relación con delitos previstos de conformidad con el presente Convenio, o cuando dicha información pueda conducir a una petición de cooperación de dicha Parte en virtud del presente Capítulo.

2. Antes de comunicar dicha información, la Parte que la proporciona podrá pedir que sea tratada de forma confidencial o que sólo se utilice bajo ciertas condiciones. Si la Parte destinataria no puede atender a dicha petición, deberá informar de ello a la otra Parte, que decidirá a continuación si, no obstante, debe proporcionar la información. Si la Parte destinataria acepta la información bajo las condiciones establecidas, estará obligada a respetarlas.

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

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

1. En ausencia de tratado de asistencia mutua o de acuerdo basado en legislación uniforme o recíproca en vigor entre la Parte requirente y la Parte requerida, se aplicarán las disposiciones de los párrafos 2 a 9 del presente artículo. Dichas disposiciones no se aplicarán cuando exista un tratado, acuerdo o legislación de este tipo, a menos que las Partes implicadas decidan aplicar en su lugar la totalidad o una parte del resto del presente artículo.

2. a. Cada Parte designará una o varias autoridades centrales encargadas de enviar las solicitudes de asistencia mutua o de responder a las mismas, de ejecutarlas o de remitirlas a las autoridades competentes para su ejecución;

b. las autoridades centrales comunicarán directamente entre sí;

c. en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, cada Parte comunicará al Secretario General del Consejo de Europa los nombres y direcciones de las autoridades designadas en aplicación del presente párrafo.

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

3. Las solicitudes de asistencia mutua en virtud del presente artículo se ejecutarán de conformidad con el procedimiento especificado por la Parte requirente, salvo cuando dicho procedimiento sea incompatible con la legislación de la Parte requerida.

4. Además de las condiciones o los motivos de denegación previstos en el párrafo 4 del artículo 25, la asistencia mutua puede ser denegada por la Parte requerida:

a. si la solicitud tiene que ver con un delito que la Parte requerida considera de carácter político o vinculado a un delito de carácter político; o
b. si la Parte requerida estima que acceder a la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.

5. La Parte requerida podrá aplazar su actuación en respuesta a una solicitud si dicha actuación puede perjudicar a investigaciones o procedimientos llevados a cabo por sus autoridades.

6. Antes de denegar o aplazar su cooperación, la Parte requerida estudiará, previa consulta con la Parte requirente cuando proceda, si puede atenderse la solicitud parcialmente o bajo las condiciones que considere necesarias.

7. La Parte requerida informará rápidamente a la Parte requirente del curso que prevé dar a la solicitud de asistencia. Deberá motivar toda denegación o aplazamiento de la misma. La Parte requerida informará asimismo a la Parte requirente de cualquier motivo que imposibilite la ejecución de la asistencia o que pueda retrasarla sustancialmente.

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

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

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

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

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

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

**Artículo 28 – Confidencialidad y restricciones de uso**

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

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

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

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

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

**Sección 2 – Disposiciones específicas**

*Título 1 – Asistencia mutua en materia de medidas provisionales*

**Artículo 29 – Conservación rápida de datos informáticos almacenados**

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

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

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

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

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

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

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

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

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

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

**Artículo 30 – Revelación rápida de datos conservados**

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

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

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

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

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

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

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

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

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

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

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

Una Parte podrá, sin autorización de otra:

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

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

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

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

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

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

*Título 3 – Red 24/7*

**Artículo 35 – Red 24/7**

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

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

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

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

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

**Capítulo IV – Cláusulas finales**

**Artículo 36 – Firma y entrada en vigor**

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

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

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

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

**Artículo 37 – Adhesión al Convenio**

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

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

**Artículo 38 – Aplicación territorial**

1. En el momento de la firma o del depósito del instrumento de ratificación, aceptación, aprobación o adhesión, todo Estado podrá designar el territorio o los territorios a los que se aplicará el presente Convenio.

2. Posteriormente, todo Estado podrá, en cualquier momento y por medio de una declaración dirigida al Secretario General del Consejo de Europa, hacer extensiva la aplicación del presente Convenio a cualquier otro territorio especificado en la declaración. El Convenio entrará en vigor respecto de dicho territorio el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido la declaración.

3. Toda declaración formulada en virtud de los dos párrafos precedentes podrá ser retirada, respecto de cualquier territorio especificado en la misma, mediante notificación dirigida al Secretario General del Consejo de Europa. La retirada surtirá efecto el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido la notificación.

**Artículo 39 – Efectos del Convenio**

1. El objeto del presente Convenio es completar los tratados o acuerdos multilaterales o bilaterales aplicables entre las Partes, incluidas las disposiciones:

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

– del Convenio Europeo de Asistencia Judicial en Materia Penal, abierto a la firma el 20 de abril de 1959 en Estrasburgo (STE nº 30),

– del Protocolo adicional al Convenio Europeo de Asistencia Judicial en Materia Penal, abierto a la firma el 17 de marzo de 1978 en Estrasburgo (STE nº 99).

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

3. Nada de lo dispuesto en el presente Convenio afectará a otros derechos, restricciones, obligaciones y responsabilidades de cada Parte.

**Artículo 40 – Declaraciones**

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

**Artículo 41 – Cláusula federal**

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

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

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

**Artículo 42 – Reservas**

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

**Artículo 43 – Mantenimiento y retirada de las reservas**

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

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

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

**Artículo 44 – Enmiendas**

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

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

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

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

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

**Artículo 45 – Solución de controversias**

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

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

**Artículo 46 – Consultas entre las Partes**

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

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

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

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

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

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

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

**Artículo 47 – Denuncia**

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

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

**Artículo 48 – Notificación**

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

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

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

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

MINISTERIO DE RELACIONES EXTERIORES

***MUY URGENTE***

# MEMORÁNDUM (DCT) Nº DCT0122/2017

**A** : DIRECCIÓN GENERAL DE TRATADOS

**De** : DIRECCIÓN DE CIENCIA Y TECNOLOGÍA

**Asunto** : Se solicita inicio del perfeccionamiento interno para la adhesión del Perú al Convenio de Budapest sobre Ciberdelincuencia

---

Se tiene a bien solicitar a la Dirección General a su cargo, el inicio del proceso de perfeccionamiento interno para la adhesión del Perú al Convenio de Budapest sobre Ciberdelincuencia, en adelante, el Convenio.

Como es de su conocimiento, el Convenio es un tratado multilateral adoptado en el seno del Consejo de Europa, el 23 de noviembre de 2001 en Budapest en idiomas inglés y francés, y entró en vigor el 01 de julio de 2004.

El Convenio tiene como la finalidad establecer reglas de cooperación internacional para que los países miembros puedan hacer frente a esta nueva amenaza mediante la armonización de sus leyes nacionales y la optimización de técnicas de investigación, contiene compromisos de carácter programático (capítulos I y II) y de asistencia judicial internacional (capítulo III).

Luego de un largo proceso de negociación a cargo de esta Cancillería, el Perú fue invitado formalmente a adherirse al Convenio en febrero de 2015. Es así que esta Dirección procedió a solicitar las opiniones favorables de los sectores competentes en la materia (Ministerio de Justicia, Poder Judicial , Secretaria de Gobierno Digital, Ministerio de Defensa y la Policía Nacional del Perú).

Como parte del procedimiento de consultas, se acordó con los mencionados sectores la suscripción de un Acta de Reunión Multisectorial en donde se plasme la conformidad de todos ellos en que el Perú se adhiera al Convenio y el encargo al Ministerio de Justicia el coordinar con esta Cancillería el texto final de las declaraciones y reservas que formulará el Perú al momento de la adhesión al Convenio.

La adhesión del Perú al Convenio, resulta importante y necesaria, toda vez que ayudará a prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como su abuso; garantizando la tipificación como delito de dichos actos, facilitando su detección, investigación y posterior sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones que permitan una cooperación judicial internacional rápida y fiable.

94

Asimismo, la adhesión al Convenio permitirá al Perú aplicar a programas técnicos y de capacitación sobre Ciberdelincuencia y temas afines. A su vez, se beneficiará de la cooperación entre los países parte del Convenio.

Por todo lo expuesto, esta Dirección considera que al incorporarnos en breve al Convenio de Budapest, nuestro país será pionero en la región latinoamericana en la lucha frontal contra la Ciberdelincuencia y con ello lograr que el Perú, y particularmente su sistema judicial, pueda beneficiar a todos los peruanos a través de las herramientas que pone a nuestra disposición el Convenio de Budapest sobre Ciberdelincuencia.

Es importante señalar, que esta Dirección ha desplegado sus mejores esfuerzos para que la adhesión al Convenio sea realizada de la forma más expeditiva posible.

Asimismo, es de destacar que la próxima adhesión del Perú al Convenio, será propuesta para que sea incluida en el mensaje a la nación con ocasión del 28 de julio, a cargo del Señor Presidente Pedro Pablo Kuczynski.

Finalmente, se adjunta las opiniones técnicas favorables del Ministerio de Justicia, sector clave para la aplicación del Convenio, el Acta de la reunión multisectorial que contiene la conformidad de los sectores concernidos por el Convenio, la propuesta de Declaraciones y Reservas a ser formuladas por el Estado Peruano y el texto íntegro del Convenio de Budapest, para los fines correspondientes.

Lima, 12 de junio del 2017

María Milagros Castañon Seoane
Ministra
Directora de Ciencia y Tecnología

C.C:DGT; DGT; DGT; EPT; DCT
RACC

Con Anexo(s) : DOC043.pdf DOC042.pdf DOC040.pdf DOC039.pdf DOC038.pdf

Propuesta de Declaraciones y Reservas del Perú al Convenio de Budapest.docx

Convenio de Budapest- versión Español.pdf

Proveido de Jorge Alejandro Raffo Carbajal ( 12/06/2017 04:16:20 pm )
Derivado a Fiorella Nalvarte :

95

SECRÉTARIAT GÉNÉRAL

DIRECTION DU CONSEIL JURIDIQUE
ET DU DROIT INTERNATIONAL PUBLIC (JURISCONSULTE)
DIVISION DU DROIT INTERNATIONAL PUBLIC
ET DU BUREAU DES TRAITES

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Référence à rappeler: JJ003/2015
AG/ik

*Strasbourg, le 20 février 2015*

*Madame l'Ambassadeur,*

*J'ai le plaisir de faire suite à votre lettre du 8 septembre faisant part du souhait du Gouvernement du Pérou d'être invité à adhérer à la Convention sur la cybercriminalité (STE n° 185), en vous informant que le Comité des Ministres du Conseil de l'Europe a décidé, lors de la 1220e réunion des Délégués des Ministres du 18 février 2015, d'inviter le Pérou à adhérer ladite Convention conformément à son article 37, paragraphe 1.*

*Conformément aux décisions des Délégués des Ministres du 10 avril 2013 (1168e réunion) relatives au passage en revue des conventions du Conseil de l'Europe, la décision d'inviter le Pérou à adhérer à la Convention sur la cybercriminalité est valide cinq ans à compter de son adoption.*

*Je me félicite de cette décision du Comité des Ministres qui souligne l'importance d'une coopération internationale contre les infractions commises au travers d'internet et d'autres réseaux informatiques.*

*Le Bureau des Traités du Conseil de l'Europe se tient à votre disposition pour toute information que vous souhaiteriez recevoir en vue d'organiser à Strasbourg le dépôt de l'instrument d'adhésion à la Convention par le Pérou.*

*Je vous prie d'agréer, Madame l'Ambassadeur, l'assurance de ma haute considération.*

*Pour le Secrétaire Général*
*Jörg POLAKIEWICZ*
*Directeur du Conseil juridique*
*et du Droit international public*

*Madame Cristina Laboureix*
*Ambassadeur du Pérou en France*

96

Conseil de l'Europe
F-67075 Strasbourg Cedex
Tél.: +33 (0)3 88 41 20 00

Bureau des Traités: +33 (0)3 90 21 43 18
+33 (0)3 88 41 36 68
Fax: +33 (0)3 90 21 51 31

E-mail: treaty.office@coe.int
http://conventions.coe.int

PERÚ | Ministerio de Justicia y Derechos Humanos | Despacho Viceministerial de Justicia | Dirección General de Asuntos Criminológicos

"Año del buen servicio al ciudadano"

Miraflores, 18 AGO. 2017

**OFICIO N° 149 -2017-JUS/DGAC**

Señora Ministra
**MILAGROS CASTAÑON SEOANE**
Directora de la Dirección de Ciencia y Tecnología
Ministerio de Relaciones Exteriores
Jirón Lampa 580, Distrito de Lima
Presente.-

Asunto : Remite Informe reservas y declaraciones que se formularán al Convenio de Budapest

Referencia : Resolucion Ministerial N° 0086-2017 de fecha 19 de abril de 2017.

De mi mayor consideración:

Es grato dirigirme a usted para saludarla cordialmente y, a la vez, en atención a la comunicación electrónica de la fecha, a través de la cual la la Dirección de Ciencia y Tecnología del Ministerio de Relaciones Exteriores solicita el pedido de informe sobre las reservas y declaraciones que se formularán al Convenio de Budapest, remitir los siguientes documentos: i) Informe Usuario N° 14-2017-JUS/DGAC de fecha 18 de agosto de 2017, elaborado por la abogada especialista Eliana Carbajal Lovatón; u ii) Propuesta de Declaraciones y Reservas del Perú al Convenio de Budapest, debidamente visada.

Sin otro particular, hago propicia la ocasión para reiterarle mi consideración y alta estima.

Atentamente,

Ministerio de Justicia y Derechos Humanos
DIRECCION GENERAL DE ASUNTOS CRIMINOLÓGICOS

VICTOR MANUEL QUINTEROS MARQUINA
Director General
Dirección General de Asuntos Criminológicos
MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS

ecl/VMQM

97

"Año del buen servicio al ciudadano"

**INFORME USUARIO Nº 14 -2017-JUS/DGAC**

**A** : **Dr. VICTOR QUINTEROS MARQUINA**
Director de la Dirección General de Asuntos Criminológicos

**ASUNTO** : Informe Complementario sobre declaraciones y reservas al Convenio de Budapest sobre Ciberdelincuencia

**REFERENCIA** : Proveído N° 1097-2017-JUS/VMJ
OF. N° 3163-2017-DP/SSG
Oficio RE (DAE-DCT) N° 2-19-A/39
Oficio RE (DAE-DCT) N° 2-19-A/16
Oficio RE (DAE-DCT9 N° 2-19-B/146
Informe N° 053-2015-JUS/DGPCP
Informe N° 071-2016-JUS/DGPCP

MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS
Dirección General de Asuntos Criminológicos
18 AGO. 2017
RECIBIDO
Hora
Firma
N° REGISTRO

**FECHA** : Miraflores, 18 de agosto de 2017

---

Tengo a bien dirigirme a usted, en atención al documento de la referencia, informarle lo siguiente:

## I.- ANTECEDENTES. -

1.1. El Convenio sobre ciberdelincuencia o cibercrimen, también conocido como el Convenio de Budapest sobre ciberdelincuencia o simplemente como Convenio Budapest, es el único acuerdo internacional que cubre todas las áreas relevantes de la legislación sobre ciberdelincuencia (derecho penal, derecho procesal y cooperación internacional) y trata con carácter prioritario una política penal contra la ciberdelincuencia.

1.2. El Comité de Ministros del Consejo de Europa en su sesión número 109 del 8 de noviembre de 2001, aprobó el Convenio y su Informe Explicativo. El 23 de noviembre de ese mismo año, se abrió a la firma en Budapest y entró en vigor el 1 de julio de 2004. A partir del 28 de octubre de 2010, 30 Estados firmaron, ratificaron y se adhirieron a la Convención, mientras que otros 16 estados firmaron la Convención, pero no la ratificaron. Actualmente nuestro país ha basado su ley de delitos informáticos[1] en este Convenio y a la fecha, a través de la Cancillería de la República, viene realizando el proceso de perfeccionamiento interno a fin de adherirse al mismo, en tanto, constituye el único documento que se encarga de la seguridad de la información y trata los delitos contra la Confidencialidad, Integridad y Disponibilidad de los datos y los sistemas informáticos.

[1] Ley N° 30096, publicada en el diario oficial "El Peruano" el 22 de octubre del 2013. Posteriormente la citada Ley fue modificada por la Ley N° 30171, publicada en el diario oficial "El Peruano" el 10 de marzo del 2014.



98

000096



1.3. Es así, que el Ministerio de Relaciones Exteriores siguiendo el procedimiento para concretar la adhesión del Perú al Convenio sobre la Ciberdelincuencia, mediante Oficio RE (DAE-DCT) N° 2-19-A/39, de fecha 30 de abril del 2015, requirió al Ministerio de Justicia y Derechos Humanos, como ente rector en la materia, absuelva algunos puntos del proceso de perfeccionamiento interno del Convenio antes mencionado, en concordancia con la Convención de Viena sobre el derecho de los Tratados, mediante la cual se señala que a través de la adhesión *"... un estado hace constar en el ámbito internacional su consentimiento en obligarse por un tratado."* (art. 2.b).

1.4. El Ministerio de Justicia y Derechos Humanos a través de la Dirección General de Asuntos Criminológicos (antes denominada Dirección General de Política Criminal y Penitenciaria), previo a dar respuesta al requerimiento formulado por la Cancillería respecto a la absolución de algunos puntos del proceso de perfeccionamiento interno del Convenio antes mencionado, convocó y conformó un grupo multisectorial con fecha 15 de junio del año 2015, en el que participaron funcionarios del Poder Judicial, Ministerio Público, Policía Nacional del Perú y de la Oficina Nacional de Gobierno Electrónico e Informática – ONGEI, a fin de presentarles el borrador del Informe dando respuesta a lo requerido por Cancillería, por lo que se procedió a recoger los comentarios y sugerencias efectuadas en la Mesa de Trabajo.

1.5. Mediante Informe N° 053-2015-JUS/DGPCP, de fecha 22 de Junio de 2015, la Dirección General de Asuntos Criminológicos (antes denominada Dirección General de Política Criminal y Penitenciaria), emitió opinión respecto a los puntos del proceso de perfeccionamiento interno del Convenio solicitado por Cancillería, concluyendo que es beneficioso para nuestro país la adhesión al mismo, en tanto, la adhesión no solo llena un vacío para el Perú, sino para toda la región latinoamericana, lo que posibilitará la Cooperación Internacional mutua entre el Perú y los países desarrollados en la materia, con la finalidad de investigar, procesar y sancionar dichos delitos. Asimismo, la adhesión permitirá al Perú solicitar la ayuda técnica al Consejo de Europa, conforme lo ha hecho con los demás países adheridos.

1.6. Mediante Oficio RE (DAE-DCT) N° 2-19-A/16, de fecha 11 de abril del año 2016, el Viceministro de Relaciones Exteriores, atendiendo que con fecha 06 de octubre del año 2015, los sectores nacionales concernidos expresaron su conformidad con las reservas y declaraciones formuladas por esta Dirección General en el Informe N° 053-2015-JUS/DGPCP; procedió a remitir las recomendaciones planteadas a efectos de que sean validadas.

1.7. Mediante Informe N° 071-2016-JUS/DGPCP, de fecha 19 de abril del año 2016, la Dirección General de Asuntos Criminológicos, concluye que las recomendaciones planteadas han sido recogidas en su totalidad en las Declaraciones a efectuarse al momento del depósito del instrumento de adhesión del Perú al Convenio de Budapest, por lo que procede a validar las mismas; y señala además que, se verifica que nuestra legislación nacional, se adapta en lo referente a lo dispuesto en los artículos 16 a 21 del Convenio de Budapest, cumpliendo de ésta manera las disposiciones de cooperación internacional.

99

1.8. Mediante Oficio RE (DAE-DCT9 N° 2-19-B/146, de fecha 29 de marzo del año 2017, la Dirección de Ciencia y Tecnología del Ministerio de Relaciones Exteriores convoca a una reunión de trabajo con la finalidad de concretar los últimos pasos del perfeccionamiento interno de la adhesión del Perú al Convenio de Budapest.

1.9. Con fecha 31 de marzo de 2017, se llevó a cabo en el Ministerio de Relaciones Exteriores, la reunión multisectorial de coordinación en torno a la adhesión del Perú al Convenio de Budapest sobre Ciberdelincuencia, con el objetivo de evaluar y brindar su conformidad al proceso de adhesión del Perú al referido Convenio.

1.10. En la citada reunión participaron funcionarios representantes de la Dirección General de Asuntos Criminológicos del Ministerio de Justicia y Derechos Humanos, de la Secretaría de Gobierno Digital de la Presidencia de Consejo de Ministros; Secretaría de Seguridad y Defensa Nacional del Ministerio de Defensa; Policía Nacional del Perú; Ministerio Público, Poder Judicial y de la Dirección de Ciencia y Tecnología del Ministerio de Relaciones Exteriores, expresando los sectores presentes su total conformidad y reiteran su opinión favorable a la adhesión del Perú al Convenio.

1.11. Mediante comunicación electrónica de fecha 20 de abril del año en curso, la Dirección de Ciencia y Tecnología del Ministerio de Relaciones Exteriores, procede a remitir el Acta de Reunión Multisectorial de Coordinación sobre Adhesión del Perú al Convenio de Budapest sobre ciberdelincuencia, llevada a cabo el día 31 de marzo del año en curso, a efectos de que la Dirección General de Política Criminal y Penitenciaria y los demás sectores nacionales concurrentes procedan a rubricar la misma.

1.12. Mediante comunicación electrónica de la fecha, la Dirección de Ciencia y Tecnología del Ministerio de Relaciones Exteriores, solicita emitir un Informe Complementario respecto a las declaraciones y reservas al Convenio de Budapest sobre Ciberdelincuencia, en atención a los Informes emitidos por esta Dirección General.

## II.- ANÁLISIS. -

### 2.1.- Declaraciones conforme al artículo 40 del Convenio:

De acuerdo a lo regulado por el artículo 40° del Convenio referido a la facultad que tienen los Estados de "(...) declarar, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, que se acoge a la facultad de exigir, llegado el caso, uno o varios elementos complementarios previstos en los artículos 2, 3, 6. 1b), 7, 9.3 y 27.9 e)", se recomienda acoger esta facultad y por lo tanto, se formule las declaraciones correspondientes a los siguientes artículos conforme al siguiente detalle que se propone:

**Artículo 2, Acceso ilícito:**
*"Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático. Cualquier Parte*

*podrá exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático".*

**Propuesta de texto de declaración:**
*"De conformidad con lo dispuesto en el artículo 2 del Convenio sobre la Ciberdelincuencia, la República del Perú declara que su legislación exige que el delito de acceso ilícito se cometa infringiendo medidas de seguridad".*

Se considera oportuno la formulación de dicha declaración en la medida que nuestra legislación ha tomado el elemento complementario del artículo 2° de la exigencia de la comisión por vulneración de medidas de seguridad. En este sentido, el Estado peruano debe acoger la facultad de exigir dicho elemento como complementario.

**Artículo 3, Interceptación ilícita:**
*"Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos. Cualquier Parte podrá exigir que el delito se haya cometido con intención delictiva o en relación con un sistema informático conectado a otro sistema informático".*

***Propuesta de texto de declaración:***
*"De conformidad con lo dispuesto en el artículo 3 del Convenio sobre la Ciberdelincuencia, la República del Perú declara que su legislación exige que el delito de interceptación ilícita* ***se cometa*** *con intención delictiva y que dicho delito* ***puede cometerse*** *en relación con un sistema informático conectado a otro sistema informático".*

Se recomienda la formulación de dicha declaración, en la medida que el delito de interceptación ilícita se encuentra recogido en la Ley de Delitos Informáticos con el nomen iuris: "Interceptación de datos informáticos", bajo la siguiente redacción:

**"Artículo 7. Interceptación de datos informáticos**
El que deliberada e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidos a un sistema informático, originados en un sistema informático o efectuado dentro del mismo que transporte dichos datos informáticos, será reprimido con una pena privativa de libertad no menor de tres ni mayor de seis años.

La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la Información Pública.

La pena privativa de libertad será no menor de ocho ni mayor de diez cuando el delito comprometa la defensa, seguridad o soberanía nacionales.

Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta un tercio por encima del máximo legal previsto en los supuestos anteriores".

El artículo 3° del Convenio de Budapest tiene en su parte final dos (02) elementos complementarios. El primero de ellos es la "exigencia de la comisión con intención delictiva" que nuestra legislación si ha tomado en consideración, al configurar la figura como dolosa. Respecto al segundo elemento: "la exigencia de la comisión en relación con un sistema informático conectado a otro sistema informático", esta modalidad de comisión de este delito, se subsume dentro de la descripción del tipo penal peruano. En tal medida, de conformidad con la facultad establecida en el artículo 40° del Convenio de Budapest, se recomienda formular una declaración al mencionado artículo conforme al detalle señalado en párrafos anteriores.

**Art. 7, Falsificación informática:**
*"Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno, cuando se cometa de forma deliberada e ilegítima, la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles. Cualquier Parte podrá exigir que exista una intención fraudulenta o una intención delictiva similar para que se considere que existe responsabilidad penal".*

Sobre el particular, el supuesto que regula el mencionado artículo, supone un concurso real conocido en la dogmática como concurso medial, por el cual existe un delito medio (que en el caso en concreto es un daño informático) y un delito fin (que en este caso en particular, se trata de la utilización de datos no auténticos con efectos legales como auténticos), unidos por una conexión lógica criminal, la necesidad del primero para configurar el segundo.

En tal sentido, esta modalidad se utiliza para sancionar el delito medio sin la necesidad de que se configure el delito fin, bastando la tentativa del primero para su consumación. Se trata, entonces, de una forma genérica de daños informáticos, que incluye una finalidad ulterior, y solo es posible su tipificación bajo una circunstancia agravante.

Por lo expuesto, se considera importante que el Estado peruano acoja la facultad de exigir dicho elemento complementario, en tanto el Estado pueda posteriormente, regular dicha conducta en un futuro.

***Propuesta de texto de declaración:***
"De conformidad con lo dispuesto en el artículo 7 del Convenio sobre la Ciberdelincuencia, la República del Perú declara que podrá exigir que exista una intención fraudulenta o delictiva similar, conforme a lo establecido en su derecho interno, para que las conductas descritas en dicho artículo generen responsabilidad penal".

**Artículo. 27, Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables:**

*"9. e) En el momento de la firma o el depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, cada Parte podrá informar al Secretario General del Consejo de Europa de que, por razones de eficacia, las solicitudes formuladas en virtud del presente apartado deberán dirigirse a su autoridad central".*

El elemento complementario del mencionado artículo, establece la prerrogativa del Estado peruano a informar, cuando se trata de asistencia mutua con carácter de urgencia, al secretario general del Consejo de Europa, en aras de la eficacia de la cooperación internacional en la lucha frente al ciberdelito, que las solicitudes formuladas en virtud de dicho carácter de urgencia deberán dirigirse directamente a la autoridad central del Perú y no a las autoridades homologas de la parte requirente.

Al respecto, la legislación nacional, conforme al Nuevo Código Procesal Penal, promulgado por Decreto Legislativo N° 957, en el artículo 512° establece que la Autoridad Central para temas de cooperación judicial internacionales es la Fiscalía de la Nación. Esta es la regla en nuestra legislación interna. Tomando en consideración ello, ese considera necesario formular una declaración al referido artículo en donde se deje en claro de forma expresa que las solicitudes efectuadas en virtud de lo dispuesto en el numeral 9 del Convenio, deberá dirigirse a su autoridad central, es decir, para el caso peruano, la Fiscalía de la Nación.

***Propuesta de texto de declaración:***
"De conformidad con lo establecido en el artículo 27, numeral 9, literal e) del Convenio sobre la Ciberdelincuencia, la República del Perú declara que, en aras de la eficacia, las solicitudes efectuadas en virtud de lo dispuesto en el numeral 9 del Convenio deberán dirigirse a su autoridad central".

**2.2.- <u>Reservas conforme al artículo 42 del Convenio</u>:**

De conformidad con lo establecido en el artículo 42 ° del Convenio sobre la facultad de formular reservas al párrafo 2 del artículo 4°, el párrafo 3 del artículo 6, el párrafo 4 del artículo 9, el párrafo 3 del artículo 10, el párrafo 3 del artículo 11

**<u>Artículo 6, Abuso de los dispositivos:</u>**

*"3. Cualquier Parte podrá reservarse el derecho a no aplicar lo dispuesto en el apartado 1 del presente artículo, siempre que la reserva no afecte a la venta, la distribución o cualquier otra puesta a disposición de los elementos indicados en el apartado 1.a.ii) del presente artículo".*

**Propuesta de texto de reserva:**
*"De conformidad con lo dispuesto en el párrafo 3 del artículo 6 del Convenio sobre la Ciberdelincuencia, la República del Perú se reserva el derecho de no aplicar el artículo 6, párrafo 1, literal b del Convenio".*

Se considera necesario la formulación de la mencionada reserva, en la medida que nuestra legislación interna en la materia no regula dicho supuesto.

**Artículo. 9, Delitos relacionados con la pornografía infantil:**

*"4. Cualquier Parte podrá reservarse el derecho a no aplicar, en todo o en parte, las letras d) y e) del apartado 1, y las letras b) y c) del apartado 2".*

**Propuesta de texto de reserva:**

*"De conformidad con el numeral 4 del artículo 9° del Convenio sobre la Ciberdelincuencia, la República del Perú considera que el bien jurídico tutelado en el derecho interno con respecto a la pornografía infantil es la libertad y/o indemnidad sexual de un menor, por lo que formula una reserva a los literales b) y c) del párrafo 2 del citado artículo, debido a que las conductas contempladas en dichas disposiciones no involucran la participación de un menor de edad".*

Sobre el particular, la reserva se plantea sobre los apartados b) y c).

En torno al literal b), en él se regula el supuesto de pornografía simulada, es decir, donde no existe participación de menores de edad. Este supuesto no regula los bienes jurídicos que protege la pornografía infantil en nuestra legislación, estos son, la libertad y/o indemnidad sexual. Por tal motivo, se considera necesario que el Estado peruano formule una reserva a dicho literal, en la medida que nuestro ordenamiento jurídico no acoge esta modalidad de delito.

En torno al literal c), en él se regula la denominada "pornografía infantil técnica o artificial". En ese sentido, en la línea del argumento anterior, al no involucrarse a un menor para la comisión del delito, nuestra legislación en la materia no regula dicho supuesto. Por tal motivo, se considera necesario la formulación de una reserva a dicho literal.

**Artículo. 29, Conservación rápida de datos informáticos almacenados:**

*"4. Cuando una Parte exija la doble tipificación penal como condición para atender una solicitud de asistencia mutua para el registro o el acceso de forma similar, la confiscación o la obtención de forma similar o la revelación de datos almacenados, dicha Parte podrá reservarse, en relación con delitos distintos de los previstos con arreglo a los artículos 2 a 11 del presente Convenio, el derecho a denegar la solicitud de conservación en virtud del presente artículo en los casos en que tenga motivos para creer que la condición de la doble tipificación penal no podrá cumplirse en el momento de la revelación".*

**Propuesta de texto de reserva:**

*"Conforme al numeral 4 del artículo 29 del Convenio sobre la Ciberdelincuencia, la República del Perú se reserva el derecho a denegar la solicitud de conservación en virtud de dicho artículo en el caso que tenga motivos para creer que, en el momento de la revelación de los datos, no se cumplirá con la condición de la doble tipificación penal".*

Sobre el particular, nuestra legislación contempla la "doble incriminación" como tutela interna al proceso de extradición, de conformidad con el artículo 517° del Código Procesal Penal aprobado por Decreto Legislativo N° 957. En tal sentido, se considera necesario la formulación de una reserva al mencionado artículo.

**III.- CONCLUSIONES. -**

Estando a lo expuesto, la Dirección General de Asuntos Criminológicos, reitera la formulación de reservas y declaraciones consignadas en el presente documento, anotando que en relación a los demás artículos regulados en el Convenio de Budapest, estos se encuentran en concordancia con nuestro ordenamiento interno en la materia, por lo que no se considera necesario la formulación de declaración o reserva adicional a las ya mencionadas en el presente documento.

Es todo cuanto informó a usted para los fines que estime por conveniente.

Atentamente,

**Abog. ELIANA CARBAJAL LOVATON**
Dirección General de Asuntos Criminológicos

105

# Propuesta de Declaraciones y Reservas del Perú al Convenio de Budapest

## I. DECLARACIONES CONFORME AL ARTÍCULO 40 DEL CONVENIO:

**Art. 2, Acceso ilícito:** *"Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático. Cualquier Parte podrá exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático".*

*Propuesta de texto de declaración:*

*"De conformidad con lo dispuesto en el artículo 2 del Convenio sobre la Ciberdelincuencia, la República del Perú declara que su legislación exige que el delito de acceso ilícito se cometa infringiendo medidas de seguridad".*

**Art. 3, Interceptación ilícita:** *"Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos. Cualquier Parte podrá exigir que el delito se haya cometido con intención delictiva o en relación con un sistema informático conectado a otro sistema informático".*

*Propuesta de texto de declaración:*

"De conformidad con lo dispuesto en el artículo 3 del Convenio sobre la Ciberdelincuencia, la República del Perú declara que su legislación exige que el delito de interceptación ilícita se cometa con intención delictiva y que dicho delito puede cometerse en relación con un sistema informático conectado a otro sistema informático".

**Art. 7, Falsificación informática:**

*"Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno, cuando se cometa de forma deliberada e ilegítima, la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles. Cualquier Parte podrá exigir que exista una intención fraudulenta o una intención delictiva similar para que se considere que existe responsabilidad penal".*

*Propuesta de texto de declaración:*

"De conformidad con lo dispuesto en el artículo 7 del Convenio sobre la Ciberdelincuencia, la República del Perú declara que podrá exigir que exista una intención fraudulenta o delictiva similar, conforme a lo establecido en su derecho interno, para que las conductas descritas en dicho artículo generen responsabilidad penal".

Ministerio de Justicia y Derechos Humanos
DIRECCION GENERAL DE ASUNTOS CRIMINOLÓGICOS
V. QUINTEROS M.

**Art. 27, Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables:**

*"9. e) En el momento de la firma o el depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, cada Parte podrá informar al Secretario General del Consejo de Europa de que, por razones de eficacia, las solicitudes formuladas en virtud del presente apartado deberán dirigirse a su autoridad central".*

*Propuesta de texto de declaración:*

"De conformidad con lo establecido en el artículo 27, numeral 9, literal e) del Convenio sobre la Ciberdelincuencia, la República del Perú declara que, en aras de la eficacia, las solicitudes efectuadas en virtud de lo dispuesto en el numeral 9 del Convenio deberán dirigirse a su autoridad central".

## II. RESERVAS CONFORME AL ARTÍCULO 42 DEL CONVENIO:

**Art. 6, Abuso de los dispositivos:**

*"3. Cualquier Parte podrá reservarse el derecho a no aplicar lo dispuesto en el apartado 1 del presente artículo, siempre que la reserva no afecte a la venta, la distribución o cualquier otra puesta a disposición de los elementos indicados en el apartado 1.a.ii) del presente artículo".*

Propuesta de texto de reserva:

*"De conformidad con lo dispuesto en el párrafo 3 del artículo 6 del Convenio sobre la Ciberdelincuencia, la República del Perú se reserva el derecho de no aplicar el artículo 6, párrafo 1, literal b del Convenio".*

**Art. 9, Delitos relacionados con la pornografía infantil:**

*"4. Cualquier Parte podrá reservarse el derecho a no aplicar, en todo o en parte, las letras d) y e) del apartado 1, y las letras b) y c) del apartado 2".*

Propuesta de texto de reserva:

"De conformidad con el numeral 4 del artículo 9° del Convenio sobre la Ciberdelincuencia, la República del Perú considera que el bien jurídico tutelado en el derecho interno con respecto a la pornografía infantil es la libertad y/o indemnidad sexual de un menor, por lo que formula una reserva a los literales b) y c) del párrafo 2 del citado artículo, debido a que las conductas contempladas en dichas disposiciones no involucran la participación de un menor de edad".

**Art. 29, Conservación rápida de datos informáticos almacenados:**

*"4. Cuando una Parte exija la doble tipificación penal como condición para atender una solicitud de asistencia mutua para el registro o el acceso de forma similar, la confiscación o la obtención de forma similar o la revelación de datos almacenados, dicha Parte podrá reservarse, en relación con delitos distintos de los previstos con arreglo a los artículos 2 a 11 del presente Convenio, el derecho a denegar la solicitud de conservación en virtud del presente artículo en los casos en que tenga motivos para creer que la condición de la doble tipificación penal no podrá cumplirse en el momento de la revelación".*

Propuesta de texto de reserva:

"Conforme al numeral 4 del artículo 29 del Convenio sobre la Ciberdelincuencia, la República del Perú se reserva el derecho a denegar la solicitud de conservación en virtud de dicho artículo en el caso que tenga motivos para creer que, en el momento de la revelación de los datos, no se cumplirá con la condición de la doble tipificación penal".

Ministerio de Justicia y Derechos Humanos
DIRECCIÓN GENERAL DE ASUNTOS CRIMINOLÓGICOS
V. QUINTEROS M.

*Lima 31 de marzo de 2017.*

107

PERÚ | Ministerio de Justicia y Derechos Humanos | Despacho Viceministerial de Justicia | Dirección General de Política Criminal y Penitenciaria

"Año del Buen Servicio al Ciudadano"

Miraflores, 15 MAR. 2017

10 MAY. 2017

**OFICIO Nº 584 -2017-JUS/DGPCP**

Señora
**MILAGROS CASTAÑÓN SEOANE**
Directora de Ciencia y Tecnología
Ministerio de Relaciones Exteriores
Presente.-

Asunto: Reunión de Coordinación sobre la futura adhesión del Perú al Convenio de Budapest sobre Ciberdelincuencia

Referencia: OF. RE (DAE-DCT) N° 2-19-B/85

De mi consideración:

Tengo el agrado de dirigirme a usted, para informarle algunas precisiones sobre los temas que fueron materia de consulta en el oficio de la referencia. Específicamente, se solicitó pronunciamientos de viabilidad normativa sobre los siguientes puntos:

- Artículo 12 del Convenio de Budapest
- Artículo 15 del Convenio de Budapest
- Capítulo sobre "Cooperación Internacional" del Convenio de Budapest
- Adecuaciones normativas para la implementación integra del Convenio de Budapest

Sobre el ***primer acápite*** referido al ***artículo 12 del Convenio***, debemos señalar que el Código Penal peruano en su artículo 104° y 105° regula las consecuencias accesorias que pueden recaer sobre una persona jurídica, siempre que ésta resulte vinculada o beneficiada con la comisión o encubrimiento de un delito. Si bien no se reconoce expresamente una imputación penal directa a la persona jurídica, si existe una afectación fáctica que la perjudica cuando es instrumentalizada para favorecer hechos ilícitos. El actuar por otro, contenido en el artículo 27 del Código Penal, las reglas procesales en el Código Procesal Penal del 2004, cuando se trata de delitos cometidos a través de las personas jurídicas, y los criterios jurisprudenciales contenidos en el Acuerdo Plenario N° 7-2009/CJ- 116: Personas Jurídicas y Consecuencias Accesorias, también regulan la aplicación judicial de consecuencias accesorias a una persona jurídica.

Asimismo, la Ley N° 30096, Ley de delitos informáticos, regula dos supuestos de carácter administrativo que exige a la persona jurídica brindar información sobre el levantamiento del secreto bancario (Decima Disposición Complementaria Final) y los registros de comunicaciones telefónicas (Undécima Disposición Complementaria Final), cuando así se solicite a través de una orden judicial; y que en caso de negarse la SBS y OSIPTEL, respectivamente, les aplicaran una sanción administrativa.

108

Respecto al ***artículo 15 del Convenio***, cabe señalar, que nuestra Constitución Política garantiza y salvaguarda los derechos fundamentales de los ciudadanos. En cuanto a la investigación, juzgamiento y sanción, el proceso penal peruano, cuya configuración se ha realizado dentro de un marco de Estado de Derecho, tiene relación directa con nuestra Carta Magna no sólo por constituir una norma fundamental dentro de nuestro ordenamiento jurídico, sino porque en el proceso penal todos los derechos en conflicto son fundamentales y con relevancia constitucional, como la facultad que tiene el Ministerio Público para perseguir la acción penal pública, el derecho fundamental a la libertad personal con las excepciones establecidas en la ley, la observancia del debido proceso y la tutela jurisdiccional, la presunción de inocencia, el principio de *ne bis im idem*, la publicidad en los procesos, la competencia judicial, legalidad de las medidas limitativas de derechos, la vigencia e interpretación de la ley procesal penal, legitimidad de las pruebas, la motivación de las resoluciones judiciales, el principio a no ser privado del derecho de defensa en ningún estado del proceso, el derecho de toda persona de ser informada inmediatamente de la causa o las razones de su detención, entre otros derechos y principios reconocidos constitucionalmente. Es así, que el Código Procesal Penal ha sido elaborado reconociendo garantías y derechos de las partes, pues el grado de reconocimiento de las garantías procesales del imputado y derechos del agraviado constituyen indicadores sensibles que son distintivos del tipo de democracia que rige en nuestro país[1]

Cabe indicar, que el eje de la reforma procesal penal está conformado, sin duda alguna, por las pautas de la Constitución y del Derecho Internacional de los Derechos Humanos consagrado en los tratados internacionales de derechos humanos de los que el Perú es parte, como son propiamente la Declaración Universal de Derechos Humanos, la Declaración Americana de los Derechos y Deberes del Hombre, el Pacto Internacional de Derechos Civiles y Políticos, la Convención Americana de Derechos Humanos, entre otros instrumentos garantistas, los cuales forman parte del derecho nacional en conformidad de la cláusula de incorporación del derecho internacional consagrado en el artículo 55° de la Constitución. En suma, la configuración del proceso penal según la Constitución, implica que el nuevo modelo de proceso se erige en estricta observancia de lo dispuesto por los principios y derechos fundamentales consagrados en nuestra Constitución Política, así como por lo señalado en los diversos Tratados Internacionales que forman parte del derecho nacional[2].

En relación al ***capítulo III - "Cooperación Internacional"*** y su consistencia con la normativa nacional, es de anotar que nuestra legislación nacional, conforme al Código Procesal Penal, promulgado por Decreto Legislativo N° 957, en su artículo 512°, establece que la Autoridad Central para temas de cooperación judicial internacional es la Fiscalía de la Nación. Esta es la regla en nuestra legislación interna

Al respecto, es de anotar que se solicitó la opinión técnica de la Dirección General de Justicia y Cultos, como órgano de línea especializado en promover y fortalecer las acciones de coordinación nacional e internacional con los organismos públicos y privados de todos los niveles vinculados a la justicia, a fin de consolidar la información requerida. En ese sentido,

---

[1] JURISPRUDENCIA DEL TRIBUNAL CONSTITUCIONAL. Tomo III. Ministerio de Justicia y Derechos Humanos. Secretaría Técnica Comisión Especial de Implementación del Código Procesal Penal. Colección de Referencia. Lima 2006. Pág. 51

[2] TALAVERA ELGUERA, Pablo. Comentarios al Nuevo Código Procesal Penal. Grijley, 2004. Pág. 139

precisa que del análisis realizado al Capítulo III sobre Cooperación Internacional, no se necesitarán mayores cambios sustanciales (modificación ni derogación) de darse la adhesión al Convenio, conforme se verifica del Informe N° 28-2017-JUS/DGJC-DCJI, el mismo que se adjunta a la presente.

Por último, respecto a la necesidad de adecuación normativa para la implementación íntegra del Convenio de Budapest, consideramos que no es necesaria la modificación o derogación de alguna ley, o la aprobación de medidas legislativas para la ejecución, en tanto, nuestra Constitución Política, en su artículo 55° establece que los tratados celebrados por el Estado forman parte del derecho nacional, quedando obligado automáticamente sin necesidad de ningún tipo de acto posterior de incorporación al ordenamiento interno.

Sin otro particular, hago propicia la oportunidad para reiterarle las muestras de mi consideración.

Atentamente,

VQM/vmp

MRE MESA DE PARTES RECIBIDO
CODIGO 219-1/24
Trámite a cargo de
16 MAR 2017
Copias para información
1
2
Observaciones

110

PERÚ | Ministerio de Justicia y Derechos Humanos | Despacho Viceministerial de Justicia

"Año del Buen Servicio al Ciudadano"

**INFORME N°28- 2017-JUS/DGJC-DCJI**

PARA : **PEDRO PAULINO GRÁNDEZ CASTRO**
Director General de Justicia y Cultos.

DE : **RUTH VILLEGAS MONTOYA**
Directora (e) de Cooperación Judicial Internacional

ASUNTO : Informe sobre el Capítulo III del "Convenio de Budapest sobre Ciberdelincuencia" en el proceso de perfeccionamiento interno y adhesión del Perú.

REFERENCIA : Oficio N° 252-2017-JUS/DGCP, cursado por la Dirección General de Política Criminal y Penitenciaria del MINJUS.

FECHA : Miraflores,

08 MAR. 2017

---

Tengo el agrado de dirigirme a usted,en relación al documento de la referencia, a fin de informarle lo siguiente:

## I.- ANTECEDENTES

Con Oficio N° 252-2017-JUS/DGPCP, la Dirección General de Política Criminal y Penitenciaria, remite a la Dirección General de Justicia y Cultos, el OF.RE (DAE-DCT) N° 2-19-B/85 de la Dirección de Ciencia y Tecnología del Ministerio de Relaciones Exteriores, que solicita la revisión y evaluación del capítulo III sobre Cooperación Internacional del Convenio de Budapest sobre Ciberdelincuencia– en adelante el Convenio - y su relación con la normatividad nacional.

## II.- ANÁLISIS

DIRECCIÓN DE COOPERACIÓN JUDICIAL INTERNACIONAL

2.1 El Conveniose encuentra estructurado sobre la base de un preámbulo, 48 articulos y tiene como principal objetivo el desarrollo de una política criminal a nivel internacional frente a la ciberdelincuencia, mediante la homologación de la legislación penal, sustantiva y procesal, y del establecimiento de un sistema eficaz, eficiente y en tiempo real de cooperación internacional, así como mejorar las capacidades de investigación de los delitos contemplados en dicho Convenio.

2.2 Asimismo, El Comité de Ministros del Consejo de Europa –previa consulta a los Estados contratantes – ha invitado a adheriste al Convenio a cualquier Estado que no sea miembro del Consejo de Europa (artículo 37). En este contexto, los paises de la región latinoamericana han sido invitados a adherirse al Convenio, paises como Argentina, Chile, Colombia, Costa Rica, México, Panamá, Paraguay y Perú[1].

[1] Serie de Tratados Europeos N° 185 – Convenio Sobre la Ciberdelincuencia

2 3 Respecto al capitulo III sobre Cooperación Internacional del Convenio en cuestión éste se comprende de 13 articulos (articulos del 23 al 35). El articulo 23establece los principios generales relativos a la cooperación internacional, señalando que "las Partes cooperarán entre si en la mayor medida posible de conformidad con las disposiciones del presente Capítulo, en aplicación de los instrumentos internacionales pertinentes sobre cooperación internacional en materia penal. ( )", es de precisar que esta disposición se alinea a los intereses del Estado peruano sobre la lucha contra la criminalidad, por lo que no contraviene nuestra normatividad interna.

2 4 El articulo 24 del Convenio que regula la extradición, establece en el articulo 24(1)(a) los requisitos para suconcesión, señalando que se aplicará a los delitos dispuestos en el Título 2 del Capítulo II, así también agrega, que en ambas legislaciones debe tener prevista una pena de al menos un año.

Sobre la pena prevista para la concesión de la extradición, cabe señalar que el Código Procesal Penal (modificado mediante Decreto Legislativo N° 1281) señala que será causal de rechazo de la extradición si en legislación de ambos Estados no está prevista una pena mayor o igual a dos años[2]. Sin embargo, cabe señalar que la aplicación de la normativa procesal penal interna sobre procesos de cooperación judicial internacional es supletoria, esto quiere decir, que se aplicaran en ausencia de un tratado, y, servirán para interpretar y aplicar en todo lo que no disponga en especial el tratado[3]

Esto quiere decir, que los actos de cooperación internacional se rigen por lo dispuesto en los tratados, en estos se dispondrán las causales por las cuales no será procedente la extradición, causales que pueden variar dependiendo de los intereses de los Estados negociadores. Por lo expuesto, el texto del articulo en mención no contravendría nuestra normativa interna.

DIRECCIÓN DE COOPERACIÓN JUDICIAL INTERNACIONAL

2 5 Además, el articulo 24(2) dispone que el Estado Parte considerara que los delitos definidosen los articulos 2 a 11 del Convenio estén incluidos entre los delitos que dan lugar a la extradición. Sobre ello, es de precisar que los tratados de extradición celebrados por el Estado Peruano no contempla un listado de delitos que darán lugar a la extradición, siendo de aplicación en este extremo la normativa interna para fines de la doble incriminación.

2 6 Por otro lado los articulos del 25 al 34 regulan las disposiciones que regiran para la asistencia mutua entre Estados en virtud de los delitos señalados en el Convenio.

Al respecto es de mencionar que el articulo 27 4 del Convenio agrega otros motivos (además de lo dispuesto en el articulo 25 4) para la denegatoria de asistencia mutua. Señalan que será motivo de denegatoria de asistencia mutua –

---

Articulo 517 del Codigo Procesal Penal

Articulo 508 del Codigo Procesal Penal

en virtud del Convenio- las solicitudes relacionadas con un delito de carácter político o si la solicitud atenta contra la soberanía, seguridad, orden público u otros intereses esenciales del Estado requerido. Sobre ello, el artículo 529(b) y 529(d) ya ha regulado dichos motivos como causales de denegación, por lo que no contravendría nuestra normativa.

2.7 Respecto a la asistencia mutua en medidas provisionales, el artículo 29(4) señala. "4 Cuando una Parte exige la doble tipificación penal como condición para atender a una solicitud de asistencia mutua con vistas al registro o al acceso por un medio similar, a la confiscación o a la obtención por un medio similar o a la revelación de los datos almacenados en relación con delitos diferentes de los previstos de conformidad con los artículos 2 a 11 del presente Convenio, podrá reservarse el derecho a denegar la solicitud de conservación en virtud del presente artículo en caso de que tenga motivos para creer que, en el momento de la revelación de los datos, no se cumpliera la condición de la doble tipificación penal". (Subrayado es nuestro)

Sobre el texto subrayado, es de mencionar que el Estado Peruano no requerirá realizar la reserva en mención, porque nuestra legislación interna no exige la doble tipificación penal como requisito de procedencia de la solicitud de asistencia judicial (artículo 529(2) del CPP), excepto para la presentación de solicitudes "presentadas para la práctica de bloqueos de cuentas, embargos, incautaciones o secuestro de bienes delictivos, inmovilización de activos, registros domiciliarios, allanamientos, control de comunicaciones, identificación o ubicación del producto de los bienes o los instrumentos de la comisión de un delito, y de las demás medidas limitativas de derechos". En tal sentido, al no contravenir nuestro ordenamiento interno no consideramos necesario realizar la reserva señalada.

2.8 Por último, el Art. 35 del referido Convenio, señala las Partes deberán fijar un punto de contacto localizable las 24 horas del día, y los siete días de la semana, con el fin de asegurar la asistencia inmediata en la investigación de delitos vinculados a sistemas y datos informáticos, o para obtener las pruebas en formato electrónico de un delito. De igual manera, señala que comprenderá la referida asistencia, lo cual resulta conveniente con la cooperación judicial sea más eficaz y eficiente. En lo pertinente, se recomienda que el Estado Peruano adopte las medidas necesarias para dar eficaz cumplimiento a esta disposición, a fin de no incurrir en responsabilidad internacional.

Ministerio de Justicia y Derechos Humanos
DIRECCIÓN DE COOPERACIÓN JUDICIAL INTERNACIONAL

## III.- CONCLUSIÓN

En base a lo expuesto, la Dirección de Cooperación Judicial Internacional, considera que el Capítulo III sobre Cooperación Internacional del Convenio es consistente con nuestra normatividad nacional, por lo que, en este extremo consideramos viable la adhesión al referido Convenio, la cual fortalecerá la cooperación internacional.

113

000111

PERÚ | Ministerio de Justicia y Derechos Humanos | Despacho Viceministerial de Justicia

"Año del Buen Servicio al Ciudadano"

## III.- RECOMENDACIÓN

Atendiendo a lo expuesto, se recomienda remitir el presente Informe de opinión a la Dirección de Ciencia y Tecnología del Ministerio de Relaciones Exteriores, a través de la Dirección General de Política Criminal y Penitenciaria para ser para ser sometido a su consideración.

Es todo cuanto informo a usted, salvo mejor parecer.

Atentamente,

RUTH VILLEGAS MONTOYA
Directora (e) de Cooperación Judicial Internacional
Ministerio de Justicia y Derechos Humanos

114

PERÚ | Ministerio de Relaciones Exteriores

# ACTA DE REUNIÓN MULTISECTORIAL DE COORDINACIÓN SOBRE ADHESIÓN DEL PERÚ AL CONVENIO DE BUDAPEST SOBRE CIBERDELINCUENCIA

Con fecha 31 de marzo de 2017, se llevó a cabo en el Ministerio de Relaciones Exteriores del Perú, la reunión multisectorial de coordinación en torno a la adhesión del Perú al Convenio de Budapest sobre Ciberdelincuencia, con el objetivo de evaluar y brindar su conformidad al proceso de adhesión del Perú al referido Convenio.

Participaron de la referida reunión funcionarios representantes de la Dirección General de Política Criminal y Penitenciaria del Ministerio de Justicia y Derechos Humanos, de la Secretaría de Gobierno Digital de la Presidencia de Consejo de Ministros; Secretaría de Seguridad y Defensa Nacional del Ministerio de Defensa; Policía Nacional del Perú; Ministerio Público, Poder Judicial y de la Dirección de Ciencia y Tecnología del Ministerio de Relaciones Exteriores.

Durante el desarrollo de la reunión, los sectores competentes acordaron lo siguiente:

1.- Los sectores presentes expresaron su total conformidad y reiteran su opinión favorable a la adhesión del Perú al Convenio.

2.- En relación a los beneficios de la adhesión del Perú al mencionado Convenio, los sectores manifiestan conjuntamente que resulta importante proteger a la sociedad frente a la ciberdelincuencia, ya que al ser un delito transnacional y pluriofensivo en diversos países, la adhesión al Convenio resulta ser una herramienta para complementar la legislación nacional vigente en la materia.

Es así, que en el Convenio resulta importante y necesario para prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de los mismos, garantizando la tipificación como delito de dichos actos, luchar de forma efectiva y eficaz contra dichos delitos, facilitando su detección, investigación y posterior sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones materiales que permitan una cooperación internacional rápida y fiable,

Asimismo, la adhesión al Convenio, permitirá al Perú aplicar a programas técnicos sobre Ciberdelincuencia y temas afines, patrocinados por diversas organizaciones internacionales y agencias de cooperación, tales Como el Consejo de Europa y la Organización de Estados Americanos.

A su vez, se beneficiará de la cooperación entre los países parte del Convenio, y así el Perú podrá encontrarse en mejores condiciones para combatir las infracciones contra la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos; infracciones informáticas (falsedad informática y estafa informática); infracciones relativas al contenido (pornografía infantil); entre otras.

Ministerio de Justicia y Derechos Humanos – Dirección General de Política Criminal y Penitenciaria – Quinteros M.

Rosa M. Nakayoshi Oshiro – Asesora Legal – Oficina Central de Tecnologías de la Información

Poder Judicial – Jorge del Ga... – Natalie B. Ingaruca Ruiz – Asesores

Policía Nacional del Perú – DIVINDAT – División Delitos Alta Tecnología

115

3.- Los sectores competentes concuerdan, que la legislación nacional vigente incorpora los supuestos delictivos contenidos en el Convenio de Budapest. En ese sentido, la Dirección General de Política Criminal del Ministerio de Justicia, sector competente en la materia, ha concluido que los artículos referidos a la materia son acordes con la legislación nacional vigente.

Asimismo la Dirección General de Justicia y Cultos de dicho sector, ha manifestado su conformidad con lo relativo al capítulo de Cooperación Judicial del Convenio, concluyendo que es acorde con la legislación nacional en la materia.

4.- Los sectores competentes concuerdan que la adhesión del Perú al Convenio, no requiere la derogación o modificación de leyes, ni la emisión de medidas legislativas, con rango de ley para su ejecución.

5.- Los sectores coinciden en la pertinencia de efectuar reservas y declaraciones al Convenio, por lo que acuerdan en delegar al Ministerio de Justicia la evaluación y visto bueno final a cada una de ellas. No obstante, en la presente reunión se valida la propuesta de declaraciones y reservas que el Estado Peruano formulará al Convenio.

Milagros Castañon Seoane
Directora de Ciencia y Tecnología
Ministerio de Relaciones Exteriores

Miguel del Carpio Wong
Funcionario
Secretaría de Gobierno Digital

Alicia Gamio Franco
Funcionaria
Secretaría de Gobierno Digital

Víctor Manuel Quinteros
Director General de Política Criminal y Penitenciaria
Ministerio de Justicia y Derechos Humanos

Nathalie Betsy Ingaruca Ruiz
Jefa del Gabinete de Asesores de la Presidencia del Poder Judicial
Corte Suprema de Justicia de la República

ROSA M. MATAYOSHI OSHIRO
ASESORA LEGAL
OFICINA CENTRAL DE TECNOLOGÍAS DE LA INFORMACIÓN

Rosa Matayoshi Oshiro
Asesora Legal de la Gerencia Central de Tecnologías de la Información
Ministerio Público

PERÚ | Ministerio de Relaciones Exteriores

Comandante Manuel Fabricio Guerrero Zerpa
Jefe de Departamento de Investigación de Delitos Informáticos de la División de Investigación de Delitos de Alta Tecnología
(DIVINDAT)
Policía Nacional del Perú

General Jorge Chávez Cresta
Director General de Política y Estrategia
del Ministerio de Defensa
Secretaría de Defensa Nacional - SEDENA (e)
Ministerio de Defensa

117

La firma del Señor General Jorge Chávez Cresta se da como Director General de Política y Estrategia (DIGEPE) del Ministerio de Defensa encargado de la Secretaría de Defensa Nacional (SEDENA), la cual, mediante Decreto Supremo N° 061-2016-PCM, del 15 de agosto de 2016, pasó a fusionarse a dicho sector.

MINISTERIO DE RELACIONES
EXTERIORES

# MEMORÁNDUM (DCT) Nº DCT0122/2017

| | | |
|---|---|---|
| **A** | : | DIRECCIÓN GENERAL DE TRATADOS |
| **De** | : | DIRECCIÓN DE CIENCIA Y TECNOLOGÍA |
| **Asunto** | : | Se solicita inicio del perfeccionamiento interno para la adhesión del Perú al Convenio de Budapest sobre Ciberdelincuencia |

---

Se tiene a bien solicitar a la Dirección General a su cargo, el inicio del proceso de perfeccionamiento interno para la adhesión del Perú al Convenio de Budapest sobre Ciberdelincuencia, en adelante, el Convenio.

Como es de su conocimiento, el Convenio es un tratado multilateral adoptado en el seno del Consejo de Europa, el 23 de noviembre de 2001 en Budapest en idiomas inglés y francés, y entró en vigor el 01 de julio de 2004.

El Convenio tiene como la finalidad establecer reglas de cooperación internacional para que los países miembros puedan hacer frente a esta nueva amenaza mediante la armonización de sus leyes nacionales y la optimización de técnicas de investigación, contiene compromisos de carácter programático (capítulos I y II) y de asistencia judicial internacional (capítulo III).

Luego de un largo proceso de negociación a cargo de esta Cancillería, el Perú fue invitado formalmente a adherirse al Convenio en febrero de 2015. Es así que esta Dirección procedió a solicitar las opiniones favorables de los sectores competentes en la materia (Ministerio de Justicia, Poder Judicial , Secretaria de Gobierno Digital, Ministerio de Defensa y la Policía Nacional del Perú).

Como parte del procedimiento de consultas, se acordó con los mencionados sectores la suscripción de un Acta de Reunión Multisectorial en donde se plasme la conformidad de todos ellos en que el Perú se adhiera al Convenio y el encargo al Ministerio de Justicia el coordinar con esta Cancillería el texto final de las declaraciones y reservas que formulará el Perú al momento de la adhesión al Convenio.

La adhesión del Perú al Convenio, resulta importante y necesaria, toda vez que ayudará a prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como su abuso; garantizando la tipificación como delito de dichos actos, facilitando su detección, investigación y posterior sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones que permitan una cooperación judicial internacional rápida y fiable.

118

Asimismo, la adhesión al Convenio permitirá al Perú aplicar a programas técnicos y de capacitación sobre Ciberdelincuencia y temas afines. A su vez, se beneficiará de la cooperación entre los países parte del Convenio.

Por todo lo expuesto, esta Dirección considera que al incorporarnos en breve al Convenio de Budapest, nuestro país será pionero en la región latinoamericana en la lucha frontal contra la Ciberdelincuencia y con ello lograr que el Perú, y particularmente su sistema judicial, pueda beneficiar a todos los peruanos a través de las herramientas que pone a nuestra disposición el Convenio de Budapest sobre Ciberdelincuencia.

Es importante señalar, que esta Dirección ha desplegado sus mejores esfuerzos para que la adhesión al Convenio sea realizada de la forma más expeditiva posible.

Asimismo, es de destacar que la próxima adhesión del Perú al Convenio, será propuesta para que sea incluida en el mensaje a la nación con ocasión del 28 de julio, a cargo del Señor Presidente Pedro Pablo Kuczynski.

Finalmente, se adjunta las opiniones técnicas favorables del Ministerio de Justicia, sector clave para la aplicación del Convenio, el Acta de la reunión multisectorial que contiene la conformidad de los sectores concernidos por el Convenio, la propuesta de Declaraciones y Reservas a ser formuladas por el Estado Peruano y el texto íntegro del Convenio de Budapest, para los fines correspondientes.

Lima, 12 de junio del 2017

María Milagros Castañon Seoane
Ministra
Directora de Ciencia y Tecnología

C.C:DGT; DGT; DGT; EPT; DCT
RACC

Con Anexo(s) : DOC043.pdfDOC042.pdfDOC040.pdfDOC039.pdfDOC038.pdf

Propuesta de Declaraciones y Reservas del Perú al Convenio de Budapest.docx

Convenio de Budapest- versión Español.pdf

**Proveido de Jorge Alejandro Raffo Carbajal ( 12/06/2017 04:16:20 pm )**
**Derivado a Fiorella Nalvarte :**
**Pase a la atención de la Min. Caballero y de EPT. Atte. JR**

;

119

000117

**MINISTERIO DE RELACIONES EXTERIORES**

**MEMORÁNDUM (OCJ) N° OCJ00339/2017**

**A** : DIRECCIÓN GENERAL DE TRATADOS

**De** : OFICINA DE COOPERACIÓN JUDICIAL

**Asunto** : Remite alcances relativos a la cooperación judicial internacional en el Convenio sobre la Ciberdelincuencia

---

En atención a la solicitud de esa Dirección General relacionada con los alcances del Convenio sobre la Ciberdelincuencia (en adelante el Convenio) en materia de cooperación judicial internacional, esta Oficina, en el marco de sus funciones establecidas en el Artículo 30° del Reglamento de Organización y Funciones de este Ministerio, tiene a bien señalar lo siguiente:

**[1]** El Convenio sobre la Ciberdelincuencia es un instrumento internacional adoptado en el marco del Consejo de Europa en el año 2001 en la ciudad de Budapest. Aborda la ciberdelincuencia desde la óptica del derecho penal y procesal penal, incluyendo los mecanismos de cooperación judicial internacional orientados a mejorar la colaboración sobre la materia entre los Estados Partes.

**[2]** En materia de cooperación judicial internacional, el Convenio regula, en su Capítulo III, los procedimientos de extradición y asistencia legal mutua, aspectos de gran relevancia en la persecución de los delitos informáticos, dada la universalidad de los mismos.

**[3]** En materia de extradición, el Convenio establece en su artículo 24° dos puntos importantes. *(i)* que los delitos materia del Convenio (delitos informáticos, contra la propiedad intelectual, entre otros) se consideran incluidos dentro los delitos que pueden dar lugar a la extradición, de conformidad con los Tratados sobre extradición concluidos por las Partes, comprometiéndose estas últimas a incluir dichos delitos entre los que pueden dar lugar a la extradición, en los tratados que se encuentren en negociación; y *(ii)* El Convenio podrá ser utilizado como fundamento jurídico para solicitar la extradición en caso no se cuente con ningún Tratado de extradición específico, ya sea de carácter bilateral o multilateral; respecto a los delitos materia del Convenio.

**[4]** En relación al primer punto, se entiende que el término *acuerdos concluidos*, hace referencia a *acuerdos vigentes* entre las Partes. En tal sentido, tomando en cuenta que los tratados de extradición modernos han reemplazado el listado de delitos por el requisito de la doble incriminación respecto a delitos sancionados con una determinada pena mínima en las legislaciones penales del Estado requirente y del Estado requerido; y teniendo en consideración además que el Convenio establece la obligación de los Estados Partes de tipificar como delitos dentro de su legislación interna las conductas descritas en el mismo, se colige que en el caso de que la solicitud de extradición, respecto a alguno de los delitos señalados en el Convenio, se ampare en algún Tratado bilateral o multilateral específico, el Convenio podrá ser invocado para complementar la base jurídica internacional del requerimiento.

**[5]** Lo anterior encuentra explicación en el entendido de que los Tratados bilaterales en materia de extradición, por lo general se orientan a regular el procedimiento de extradición entre los Estados que lo suscriben, sin especificar a qué delitos podría aplicarse (al margen del requisito de la pena mínima y la exclusión de delitos políticos o militares), bastando solo la doble incriminación; en cambio, los tratados de carácter multilateral por lo general se orientan a combatir cierto tipo de delitos de acuerdo al bien jurídico tutelado que deseen proteger específicamente, incluyendo mecanismos de cooperación judicial y técnica entre las Partes, ejemplo de ello son las Convenciones de las Naciones Unidas contra la corrupción, la delincuencia organizada transnacional y el tráfico de estupefacientes, así como el Convenio que nos ocupa en materia de ciberdelincuencia. En ese orden de ideas, el referido Convenio podría ser invocado en un requerimiento de extradición sobre la materia, a fin de complementar un Tratado bilateral (o multilateral cuyo objeto principal sea la extradición), pues mientras el primero recuerda el compromiso que tienen las Partes de combatir determinado delito, el segundo regula el procedimiento de extradición propiamente dicho.

120

000118

**[6]** Por el contrario, cuando no exista Tratado entre las Partes, que regule el procedimiento de extradición, el Convenio podrá ser invocado a fin de sustentar el requerimiento sobre la materia y, cualquier aspecto del procedimiento que no se encuentre regulado en el Convenio, será tratado de conformidad con la legislación interna de las Partes.

**[7]** De acuerdo a lo anteriormente señalado, se aprecia que el referido Convenio, al incluir regulaciones generales en materia de extradición, aborda implícitamente asuntos de derechos humanos y soberanía. Así, mientras la vinculación con los derechos humanos radica en el respeto a las garantías y derechos fundamentales de la persona reclamada, estableciendo las reglas para viabilizar la remisión compulsiva de un individuo solicitado en extradición, evitando la arbitrariedad de dicha remisión; la relación con la soberanía se refiere al ejercicio del *Ius puniendi* estatal, en la medida que el Estado requirente cuenta con jurisdicción respecto a los delitos cometidos en su territorio.

**[8]** Por otro lado, se precisa que el Convenio también establece una serie de medidas legislativas que los Estados Partes deberán adoptar en sus ordenamientos internos, tipificando como delitos ciertas conductas allí especificadas. En atención a ello, cabe indicar que, tomando como referente el Convenio, en el año 2013 se publicó la Ley N° 30096, Ley de Delitos Informáticos, y posteriormente, en el año 2014, la Ley N° 30171 que modifica la anterior; normativa interna que resulta compatible con el Convenio.

**[9]** Finalmente, tanto la sección referida a la extradición, como la sección referida a la asistencia legal mutua en el marco del Convenio, señalan la necesidad de designar una autoridad responsable del envío y recepción de tales requerimientos. Al respecto, como esa Dirección General conoce, la Autoridad Central peruana para la cooperación judicial internacional en materia penal, de acuerdo al artículo 512° del Código Procesal Penal, es la Fiscalía de la Nación, quien asume sus funciones a través de su Unidad de Cooperación Judicial Internacional y Extradiciones.

**[10]** Es todo cuanto se tienen a bien informar a esa Dirección General, para los fines que estime pertinentes.

Lima, 10 de julio del 2017

Elmer López Chirinos
Administrativo
Jefe de la Oficina de Cooperación Judicial

C.C: LEG,DGT,ODI
KGMC

Este documento ha sido impreso por Luis Enrique Gamero Urmeneta, quien asume la responsabilidad sobre el uso y destino de la información contenida. 16/03/18 05:01 PM

**Anexos**

***Proveidos***

Proveido de Fiorella Nalvarte (11/07/2017 08:47:54)
Derivado a María del Pilar Castro Barreda
Estimada Minisitra por indicación del Embajador Raffo pase para vuestro conocimiento y fines.
Proveido de María del Pilar Castro Barreda (11/07/2017 11:54:12)
Derivado a Luis Enrique Gamero Urmeneta
Para evaluación
Proveido de Jorge Alejandro Raffo Carbajal (11/07/2017 14:45:50)
Derivado a Luis Enrique Gamero Urmeneta
Favor urgente atención para incorporar en memo de respuesta a DCT. Atte. JR

121

000119

**MINISTERIO DE RELACIONES EXTERIORES**

***MUY URGENTE***

# MEMORÁNDUM (DCT) N° DCT00162/2017

**A** : DIRECCIÓN GENERAL DE TRATADOS

**De** : DIRECCIÓN DE CIENCIA Y TECNOLOGÍA

**Asunto** : Se remite informe del Ministerio de Justicia sobre Declaraciones y Reservas al Convenio de Budapest sobre CIberdelincuencia

**Referencia** : MEMORÁNDUM DCT01222017 y DGT06012017

---

En atención a la Memoranda de la referencia, se cumple con remitir el informe N° 149-2017-JUS/DGAC, de la Dirección General Asuntos Criminológicos , en torno a las Declaraciones y Reservas que se formularán al Convenio de Budapest sobre Ciberdelincuencia. A su vez, se anexa la propuesta de texto de declaraciones y reservas debidamente visada por dicha Dirección.

Cabe señalar que anteriormente la referida Dirección se denominaba "Dirección General de Política Criminal y Penitenciaria", la cual fue modificada mediante D.S 013-2017-JUS, Aprueban el Reglamento de Organización y Funciones del Ministerio de Justicia y Derechos Humanos, del 21 de junio de 2017.

Asimismo, esta Dirección tiene a bien precisar que, de conformidad con la normativa en materia de cooperación judicial, Código Procesal Penal -Decreto Legislativo N° 957- específicamente el artículo 512°, para todos los efectos del Convenio de Budapest, en lo que corresponde a los artículos 24.7, 27.2 y 35.1, quien ejercerá el rol de Autoridad Central, es el Ministerio Público- Fiscalía de la Nación, a través de la Unidad de Cooperación Judicial Internacional y Extradiciones (creada mediante Resolución de Fiscalía de la Nación N° 124-2006, del 3 de febrero de 2006). En ese sentido, y de conformidad con los artículos anteriormente mencionados, estará a cargo de:

- Enviar o recibir solicitudes de extradición o de detención provisional en ausencia de tratado
- Autoridad central en asistencia judicial, y
- Punto de contacto para la red 24/7

Lima, 18 de agosto del 2017

María Milagros Castañon Seoane
Ministra
Directora de Ciencia y Tecnología

C.C: EPT,DGT,DCT
RACC
Este documento ha sido impreso por Luis Enrique Gamero Urmeneta, quien asume la responsabilidad sobre el uso y destino de la información contenida. 9/13/17 10:53 AM

**Anexos**

OF. 149-2017-DGAC (2).pdf

**Proveidos**

Proveido de Fiorella Nalvarte (21/08/2017 08:39:52)
Derivado a Luis Enrique Gamero Urmeneta, Cristian Antonio Luis Pizarro
Estimados funcionarios por indicación del Embajador Jorge Raffo pase para vuestro conocimiento y fines.

122