



PRESIDENCIA DE LA REPÚBLICA DEL ECUADOR

Oficio No. T. 90-SGJ-24-0218

París, 16 de mayo de 2024

Señor Magíster
Henry Kronfle
PRESIDENTE
ASAMBLEA NACIONAL
En su despacho

De mi consideración:

DANIEL NOBOA AZÍN, Presidente Constitucional de la República comparezco ante su autoridad de conformidad a lo dispuesto en los artículos 147 numeral 10 y 418 de la Constitución de la República del Ecuador, en los siguientes términos:

I. ANTECEDENTES:

El “*Convenio sobre la Ciberdelincuencia*”, también denominado “*Convenio de Budapest*” (“Convenio”) inició su redacción en el año 1995 por el Consejo de Europa y su versión final fue aprobada en Budapest el 23 de noviembre de 2001, con entrada en vigor el 01 de julio de 2004.

El mencionado Convenio tiene como objetivo establecer una política pública a través del ámbito penal orientada a la protección de la sociedad contra la ciberdelincuencia, bajo las siguientes modalidades: i) armonizar los elementos de los delitos de conformidad con el derecho sustantivo penal de cada país y las disposiciones conexas en materia de ciberdelincuencia; ii) establecer los poderes necesarios para la investigación y el procesamiento de los delitos, así como también de otros cometidos mediante el uso de un sistema informático o las pruebas conexas que se encuentran en formato electrónico; y, iii) establecer un régimen rápido y eficaz de cooperación internacional.

La representación diplomática del Ecuador en Bruselas, mediante nota No. 4-2-070-2021 de 29 de diciembre de 2021 transmitió al Consejo de Europa, el interés del Gobierno del Ecuador de adherirse al Convenio sobre la Ciberdelincuencia. La directora de la División de Derecho Internacional Público y Oficina de Tratados del Consejo de Europa, a través de la Nota No. JJ31/2022-AG/gd de 01 de abril de 2022, informó que el Comité de Ministros del Consejo de Europa durante la sesión 1430 de 30 de marzo de 2022, extendió una invitación al Ecuador para ser parte del Convenio de Budapest.



PRESIDENCIA DE LA REPÚBLICA DEL ECUADOR

Mediante oficio No. T. 90-SGJ-24-0029 de 04 de enero de 2024, el Presidente de la República puso en conocimiento de la Corte Constitucional del Ecuador el texto del Convenio que aborda el combate a los delitos informáticos y es considerado como la norma internacional más completa en esta materia; y, solicitó emitir el dictamen correspondiente de conformidad con lo dispuesto en la Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional.

El 21 de marzo de 2024, el Pleno de la Corte Constitucional aprobó el dictamen de primer momento en el que resolvió que el Convenio requiere del pronunciamiento de la Asamblea Nacional al encontrarse incurso en el presupuesto del numeral 3 del artículo 419 de la Constitución de la República. Además, ordenó la publicación de su texto en el Registro Oficial, para que cualquier ciudadano intervenga defendiendo o impugnando su constitucionalidad.

El 02 de mayo de 2024, con oficio No. CC-SG-2024-1063, la Corte Constitucional del Ecuador notificó el Dictamen 1-24-TI/24 expedido el 25 de abril de 2024, en el cual resolvió: *“1. Declarar la constitucionalidad del ‘Convenio sobre Ciberdelincuencia’. 2. Disponer que se notifique a la Presidencia de la República el presente dictamen, a fin de que se haga conocer el mismo a la Asamblea Nacional (...)”*.

II. SOLICITUD

En virtud de lo indicado y en atención a lo dispuesto en los artículos 120 numeral 8 y 419 numeral 3 de la Constitución de la República; y, el artículo 108 numeral 6 de la Ley Orgánica de la Función Legislativa, me permito remitir por su intermedio a la Asamblea Nacional, el Convenio sobre la Ciberdelincuencia, con el propósito de que se emita la resolución correspondiente, previo a su ratificación.



Firmado electrónicamente por:
DANIEL NOBOA AZÍN
PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

Daniel Noboa Azín
PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

Adjunto:

- Copia certificada del *“Convenio sobre la Ciberdelincuencia”*.
- Dictamen 1-24-TI/24, de 25 de marzo de 2024.

Quito, D.M., 25 de abril de 2024

CASO 1-24-TI

EL PLENO DE LA CORTE CONSTITUCIONAL DEL ECUADOR, EN EJERCICIO DE SUS ATRIBUCIONES CONSTITUCIONALES Y LEGALES, EMITE EL SIGUIENTE

DICTAMEN 1-24-TI/24

Resumen: La Corte Constitucional analiza el “Convenio sobre Ciberdelincuencia” y concluye que este tratado internacional guarda conformidad con los parámetros constitucionales para la aprobación y ratificación de tratados internacionales.

1. Antecedentes

1. La representación diplomática del Ecuador en Bruselas, mediante nota 4-2-070-2021, de 29 de diciembre de 2021, transmitió al Consejo de Europa el interés del Gobierno del Ecuador de adherirse al Convenio sobre Ciberdelincuencia, conocido también como Convenio de Budapest (“**Convenio**”). La directora de la División de Derecho Internacional Público y Oficina de Tratados del Consejo de Europa, a través de la Nota JJ31/2022-AG/gd, de fecha 1 de abril de 2022, informó que el Comité de Ministros del Consejo de Europa durante la sesión 1430, de 30 de marzo de 2022, extendió una invitación al Ecuador para ser parte del Convenio de Budapest.
2. Mediante Oficio T 90-SGJ-24-0029 presentado el 05 de enero de 2024, el presidente de la República del Ecuador (“**presidente de la República**”), Daniel Noboa Azín, remitió a esta Corte Constitucional una copia certificada del Convenio y solicitó a la Corte Constitucional resolver si requiere de aprobación legislativa.
3. El 05 de enero de 2024, el sorteo para la sustanciación de la presente causa correspondió al juez constitucional Jhoel Escudero Soliz, quien avocó conocimiento el 26 de febrero de 2024.
4. El 21 de marzo de 2024, el Pleno de la Corte Constitucional aprobó el dictamen de primer momento en el que resolvió que el Convenio requiere del pronunciamiento de la Asamblea Nacional.
5. El texto del Convenio fue publicado en el Registro Oficial en la Edición Constitucional 337 del 27 de marzo de 2024. El 15 de abril de 2024, el juez sustanciador avocó conocimiento de la causa, a efectos de sustanciar el segundo momento y constató que

no se han registrado pronunciamientos de la ciudadanía, de conformidad con lo previsto en el artículo 111 numeral 2 literal b de la LOGJCC.

2. Competencia

6. El Pleno de la Corte Constitucional es competente para conocer el Tratado y emitir el dictamen sobre su constitucionalidad, de conformidad con lo dispuesto en el artículo 438 numeral 1 de la Constitución, en concordancia con los artículos 107 numeral 2, 108, 110 numeral 1 y 111 numeral 2 literal c de la LOGJCC.

3. Control automático de constitucionalidad

7. En virtud de la competencia de la Corte Constitucional para realizar un control automático de constitucionalidad de tratados e instrumentos internacionales, este Organismo procederá a realizar: i) el control formal del proceso de aprobación del Convenio y ii) el control material del contenido del Convenio bajo examen.

3.1 Control del proceso de aprobación del Convenio sobre Ciberdelincuencia

8. El artículo 147 numeral 10 de la Constitución establece que “son atribuciones y deberes de la Presidenta o Presidente de la República, además de los que determine la ley: [...] 10. Definir la política exterior, suscribir y ratificar los tratados internacionales”. En los artículos 418 y 419 de la Constitución se establece que: i) al presidente de la República le corresponde “suscribir o ratificar los tratados y otros instrumentos internacionales”; y, ii) a la Asamblea Nacional le corresponde aprobar o no, de forma previa, la ratificación o denuncia de determinados tratados internacionales.
9. Además, el artículo 438 numeral 1 de la Constitución establece que la Corte Constitucional debe emitir dictamen previo y vinculante de constitucionalidad de los tratados internacionales que requieren aprobación legislativa, previo a su ratificación por parte de la Asamblea Nacional.
10. El procedimiento para el control constitucional, que establece el artículo 438 de la Constitución, se encuentra determinado en el artículo 111 de la LOGJCC, el cual establece que el trámite seguirá las siguientes reglas:
 - a) La Presidenta o Presidente de la República enviará a la Corte Constitucional copia auténtica de los tratados internacionales, en un plazo razonable. En caso de no hacerlo, la Corte Constitucional lo conocerá de oficio.

b) Una vez efectuado el sorteo para la designación de la jueza o juez ponente, se ordenará la publicación a través del Registro Oficial y del portal electrónico de la Corte Constitucional, para que, dentro del término de diez días -contados a partir de la publicación-, cualquier ciudadano intervenga defendiendo o impugnando la constitucionalidad parcial o total del respectivo tratado internacional.

c) La Corte Constitucional deberá resolver dentro del término de treinta días contados a partir de la finalización del término para la publicación antes mencionada. En caso de no hacerlo, se entenderá que existe informe favorable de constitucionalidad, y el respectivo tratado será remitido para la aprobación legislativa.

d) En lo no previsto en este Capítulo, se seguirán las reglas determinadas para el procedimiento general

11. En relación con el Convenio bajo análisis, esta Corte verifica los siguientes aspectos relativos al proceso de aprobación de este tratado internacional:

11.1. El Convenio y su informe explicativo fueron aprobados por el Comité de Ministros del Consejo de Europa en su 109 reunión que tuvo lugar el 8 de noviembre de 2001 y fue abierto a la firma en Budapest, el 23 de noviembre de 2001, con motivo de la celebración de la Conferencia Internacional sobre la ciberdelincuencia.

11.2. La adhesión de Ecuador a dicho convenio ha sido sugerida por el Ministerio de Relaciones Exteriores y Movilidad Humana mediante oficio MREMH-MREMH-2023-0424-OF de fecha 03 de mayo de 2023, el Ministerio de Telecomunicaciones y de la Sociedad de la Información mediante oficio MINTEL-MINTEL-2021-0789-0 de fecha 20 de diciembre de 2021, la Fiscalía General del Estado mediante oficio FGE-DCAI-2021-006209-0 de fecha 6 de octubre de 2021, la Dirección Nacional de Registro de Datos Públicos mediante oficio DINARDAP-SN-2021-0003-OF de fecha 22 de septiembre de 2021, el Ministerio de Gobierno mediante MDG-VDI-SSC-2021-0167-0 de fecha 21 de septiembre de 2021, el Ministerio de Defensa mediante oficio MDN-GAB-2021-2132-OF de fecha 31 agosto de 2021, y la Policía Nacional del Ecuador mediante informe 2021-013 8-DSTIC-DNTICPN de fecha 25 agosto 2021.

11.3. La representación diplomática del Ecuador en Bruselas, mediante nota 4-2-070-2021, de 29 de diciembre de 2021, transmitió al Consejo de Europa el interés del Gobierno del Ecuador de adherirse al Convenio.

11.4. La directora de la División de Derecho Internacional Público y Oficina de Tratados del Consejo de Europa, a través de la Nota JJ31/2022-AG/gd, de fecha 1 de abril de 2022, informó que el Comité de Ministros del Consejo de Europa

durante la sesión 1430, de 30 de marzo de 2022, extendió una invitación al Ecuador para ser parte del Convenio de Budapest.

11.5. Mediante Oficio T 90-SGJ-24-0029 presentado el 05 de enero de 2024, el presidente de la República del Ecuador, Daniel Noboa Azín, remitió a esta Corte Constitucional una copia certificada del Convenio para el trámite correspondiente.

11.6. El 21 de marzo de 2024, el Pleno de la Corte Constitucional emitió el dictamen de primer momento, en el que concluyó que el presente Convenio requiere del pronunciamiento de la Asamblea Nacional.

12. El presidente de la República afirma:

El Ecuador dispone de cinco años para finalizar el proceso de adhesión al Instrumento, debiendo efectuar las enmiendas necesarias en la legislación interna, para que guarde coherencia con el Convenio de Budapest, en este período se deberá también cumplir con el procedimiento de ratificación constitucional. Concluido el procedimiento interno, el Ecuador deberá depositar el instrumento de adhesión en el Consejo de Europa. La calidad de Estado Parte será efectiva tres meses después del depósito.

13. En virtud de lo expuesto, la Corte verifica que el Convenio se encuentra abierto para la adhesión del Estado ecuatoriano, que se ha manifestado el consentimiento del Estado ecuatoriano conforme el artículo 7 literal a) Convenio de Viena sobre el Derecho de los Tratados y, en consecuencia, procedimentalmente se ha dado cumplimiento a lo establecido en los artículos 418 y 419 de la Constitución y a lo dispuesto en los artículos 111 numeral 2 literales a, b, c y d de la LOGJCC.

3.2 Control material del Convenio sobre Ciberdelincuencia

14. El artículo 108 de la LOGJCC establece: “[e]l control constitucional de los tratados internacionales comprende la verificación de la conformidad de su contenido con las normas constitucionales [...]”. A efectos del análisis que se debe realizar en este dictamen, en cada sección primero se hará una descripción del contenido y posteriormente se efectuará el análisis de constitucionalidad.

3.2.1 Preámbulo y capítulo I del Convenio

15. De manera preliminar, el Convenio está conformado por el preámbulo y 48 artículos. Su finalidad es combatir la ciberdelincuencia transnacional y la protección de datos e intimidad a través del establecimiento de una política penal común entre los Estados parte y de una cooperación internacional eficaz.

16. El Convenio inicia con el preámbulo y desarrolla su contenido en cuatro capítulos, en el que los miembros del Consejo de Europa y demás Estados signatarios expresan, entre otras motivaciones, la necesidad de aplicar una política común con el objeto de “proteger a la sociedad frente a la ciberdelincuencia, en particular mediante la adopción de una legislación adecuada y mejora de la cooperación internacional”.

17. El preámbulo señala:

...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, internacional, y estableciendo disposiciones materiales que permitan una cooperación internacional rápida y fiable.

18. El *capítulo I*, denominado “[t]erminología” está conformado por un solo artículo que contiene definiciones de: a. “sistema informático”, b. “datos informáticos”, c. “proveedor de servicios” y d. “datos relativos al tráfico”, a fin de comprender los conceptos empleados por este Convenio.

19. La Corte observa que la finalidad expresada en el preámbulo del Convenio, así como las definiciones contenidas en el capítulo I expresada en el preámbulo, no son contrarias a la Constitución y están acordes a la obligación del Estado de proteger el derecho a la intimidad¹ y facilitar el “acceso universal a las tecnologías de información y comunicación en especial para las personas y colectividades que carezcan de dicho acceso o lo tengan de forma limitada”.²

3.2.2 Capítulo II del Convenio

20. El *capítulo II* denominado “[m]edidas que deberán adoptarse a nivel nacional”, contiene tres secciones a través de las cuales se introducen elementos de Derecho Penal sustantivo, procesal y jurisdicción.

20.1. En la primera sección denominada “[d]erecho penal sustantivo”, define nueve delitos agrupados en cuatro categorías:

20.1.1. Los “[d]elitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos” el cual está conformado por los artículos 2 al 6 del Convenio que comprometen al

¹ CRE, artículo 66.20.

² CRE, artículo 17.2.

Estado a adoptar “las medidas legislativas y de otro tipo” para tipificar los delitos de: “acceso ilícito” (artículo 2), “interceptación ilícita” (artículo 3), “ataques a la integridad” (artículo 4), “ataques a la integridad del sistema” (artículo 5) y “abuso de dispositivos” (artículo 6).

20.1.2. La segunda categoría trata de los “[d]elitos informáticos” el cual está conformado por los artículos 7 y 8 del Convenio que tratan de las medidas legislativas y de otro tipo para tipificar los delitos de “falsificación informática” y “fraude informático”.

20.1.3. La tercera categoría trata de los “[d]elitos relacionados con el contenido” y está conformado por el artículo 9 que trata de las medidas legislativas y de otro tipo necesarias para la tipificación de “delitos relacionados con la pornografía infantil” conforme a los actos especificados en el Convenio. Este artículo contiene también la definición de pornografía infantil.

20.1.4. La cuarta categoría trata acerca de “[d]elitos relacionados con infracciones de la propiedad intelectual y de los derechos afines” y está conformado por el artículo 10 con tres numerales sobre medidas legislativas y de otro tipo para tipificar como delitos relacionados con infracciones a la propiedad intelectual y los derechos afines.

20.1.5. El quinto título trata de “[o]tras formas de responsabilidad y de sanción” el cual está conformado por los artículos 11, 12 y 13 del Convenio que trata sobre medidas legislativas y de otro tipo destinadas a tipificar “la complicidad deliberada” así como la tentativa, en los delitos que trata el Convenio, la responsabilidad de las personas jurídicas que incluya la imposición de sanciones o medidas penales y no penales para personas jurídicas.

21. De la revisión del Convenio se observa que este capítulo está conformado por disposiciones que obligan a los Estados parte a tipificar conductas reconocidas como ciberdelitos, para adecuar la legislación a estándares internacionales que permitan su mejor investigación y enjuiciamiento. Al respecto, esta Corte considera importante señalar que la tipificación de delitos debe orientarse a sancionar conductas penalmente relevantes que alcancen tal nivel de afectación a los derechos, bienes o valores que deban sancionarse en el ámbito penal. Así, en la aprobación de un tratado internacional de esta naturaleza, se debe tener especial atención respecto de las conductas que, al suscribirlo, el Estado ecuatoriano se compromete a incorporar en la normativa penal.

22. En virtud del examen realizado, esta Corte constata que esta sección guarda conformidad con la protección a derechos constitucionales, tales como la “intimidad personal y familiar”³ y el derecho a la inviolabilidad de la correspondencia que se reconoce en la Constitución en los siguientes términos:

el derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; esta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación.⁴

23. De manera específica el delito relacionado con la pornografía infantil contemplado en el Convenio se encuentra acorde a la protección constitucional a los niños, niñas y adolescentes, en tanto grupo de atención prioritaria y de manera específica con la obligación del estado de adoptar “(l)as políticas públicas de comunicación priorizarán su educación y el respeto a sus derechos de imagen, integridad y los demás específicos de su edad”,⁵ en orden a proteger sus derechos, en especial, su indemnidad sexual, imagen, intimidad, “a la integridad física y psíquica (y) a su identidad”.
24. En ese sentido, a efectos del análisis esta Corte toma nota del informe explicativo del Convenio de Budapest,⁶ que indica que el artículo 9 busca establecer medidas de protección para las niñas y los niños, lo que incluye su tutela contra la explotación sexual, actualizando las normas penales que permitan circunscribir de manera más efectiva el uso de sistemas informáticos en la comisión de delitos sexuales en contra de este grupo de atención prioritaria. Ello, en función de que los sistemas informáticos han transformado la producción y distribución de este delito alcanzando dimensiones internacionales, lo que exige una cooperación internacional eficaz para combatirlo y tutelar los derechos de niñas y niños.
25. De igual manera, los delitos que contempla el Convenio relativos a las infracciones de la propiedad intelectual y los derechos afines guardan conformidad con el reconocimiento constitucional de la “propiedad intelectual de acuerdo con las condiciones que señale la ley”.⁷
26. En lo relativo al delito de acceso ilícito, interceptación ilícita, ataques a la integridad del sistema, este se encuentra orientado a que el Estado proteja los derechos de

³ CRE, artículo 66.20.

⁴ CRE, artículo 66.21.

⁵ CRE, artículo 46.

⁶ El Convenio y su Informe explicativo fueron aprobados por el Comité de Ministros del Consejo de Europa en su 109ª reunión del 8 de noviembre de 2001.

⁷ CRE, artículo 322.

propiedad intelectual a través de la tipificación o la adecuación del tipo penal a las conductas que terminan por lesionar estos derechos y que se encuentran contempladas. Por ello, el Convenio guarda conformidad constitucional.

- 27.** Cabe indicar que el control que realiza la Corte Constitucional alcanza a identificar si las disposiciones de esta sección se encuentran acordes al contenido de la Constitución. Sin embargo, debido a que la tipificación de los delitos debe realizarse en la norma penal con rango de ley correspondiente, en este caso el Código Orgánico Integral Penal, de manera especial con la sección tercera que trata sobre los “delitos contra la seguridad de los activos de los sistemas de información y comunicación” que se encuentra dentro del capítulo de los delitos contra el buen vivir. También se relaciona con los artículos 103 y 104 del COIP que tipifica el delito de pornografía infantil y los artículos 208A, 208B y 208 que tipifican “actos lesivos” contra la propiedad intelectual y derechos de autor.
- 28. La sección segunda se denomina “[d]erecho procesal” y contiene cinco títulos en relación con la investigación y procesamiento de estos delitos, así como la obtención y conservación de datos y evidencia digital:**

- 28.1.1.** El primero que contiene “disposiciones comunes” conformado por el artículo 14 que trata sobre el ámbito de aplicación de las disposiciones de procedimiento y el artículo 15 que refiere a las condiciones y salvaguardias. Este último artículo en su numeral 1 expresamente señala:

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.

- 28.1.2.** Del segundo al quinto título, el Convenio prevé mecanismos que debe incorporar cada Estado parte y que permiten obtener datos para el cumplimiento del fin de este instrumento. Así, el segundo título trata sobre la “Conservación rápida de datos informáticos almacenados” y está integrado por los artículos 16 y 17. De manera expresa el numeral 1 del artículo 16 del Convenio, señala:

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.

28.1.3. El tercer título denominado “[o]rden de presentación” y está integrado por el artículo 18 relativo a medidas legislativas y de otro tipo para que las autoridades puedan, entre otras facultades, ordenar a una persona “presente en su territorio que comunique determinados datos informáticos que obren en su poder o bajo su control [...]”.

28.1.4. El cuarto título trata sobre el “[r]egistro y confiscación de datos informáticos almacenados” y está conformado por el artículo 19, cuyo contenido versa principalmente sobre medidas legislativas que deben adoptar los Estados para que las autoridades estén facultadas a tener acceso “a todo el sistema informático o parte del mismo, así como a los datos informáticos en él almacenados”. El artículo 19.4 del Convenio señala:

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.

28.1.5. El quinto título versa sobre la “[o]btención en tiempo real de datos informáticos” y está integrado por el artículo 20 que trata sobre la obligación de adoptar medidas legislativas y de otro tipo para que las autoridades se encuentren facultadas, entre otros aspectos a “obtener o grabar con medios técnicos existentes en su territorio [...] en tiempo real los datos relativos al tráfico asociados a comunicaciones específicas transmitidas en su territorio por medio de un sistema informático.” En tanto que el artículo 21 contempla la interceptación de datos relativos al contenido.

29. De la revisión de la sección segunda, se observa que en esta se establecen diferentes herramientas que buscan facilitar investigaciones penales. El Estado, al establecer, implementar y aplicar las facultades y procedimientos previstos en esta sección, debe incorporar garantías que “(...) equilibren la aplicación de estos mecanismos con la adecuada protección de los derechos humanos y las libertades”.⁸ Todo ello, en el marco de los instrumentos internacionales de derechos humanos y la aplicación del principio de proporcionalidad. La aplicación de este principio se verifica en las limitaciones

⁸ Informe explicativo del Convenio, art. 15.

previstas en los artículos 20 y 21 respecto a las obligaciones sobre las medidas de interceptación de recolección en tiempo real de datos de tráfico y datos de contenido de investigaciones circunscritas a delitos graves.

30. Cabe hacer referencia al informe explicativo del Convenio en el cual, se especifica que el artículo 15 obliga a los Estados parte a establecer condiciones y salvaguardas adecuadas para la protección de los derechos humanos y las libertades. En concreto, el Estado deberá respetar los instrumentos internacionales de derechos humanos e incorporar el principio de proporcionalidad. Sobre el principio de proporcionalidad, el informe explicativo indica que lo que persigue el Convenio es que la facultad o procedimiento sea proporcional a la naturaleza y circunstancias del delito. Otras garantías reconocidas por el Convenio en el artículo 15 son: la supervisión judicial, la motivación justificante de la aplicación, la limitación del ámbito de aplicación y la duración de la facultad o del procedimiento que se trate.
31. La sección tercera, denominada “[j]urisdicción”, se encuentra conformada por el artículo 22 que trata sobre la adopción de medidas legislativas o de otro tipo orientadas a:

... afirmar su jurisdicción respecto de cualquier delito previsto de conformidad con los artículos 2 a 11 del 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.
32. La sección segunda denominada “derecho procesal” y la sección tercera denominada “jurisdicción” se relacionan con el proceso de juzgamiento de los delitos de ciberdelincuencia que contempla el Convenio. Revisados los artículos que comprenden estas secciones, no se verifica que estas limiten o se encuentren en contraposición con el derecho al debido proceso y el derecho a la defensa reconocidos en los artículos 76 y 77 de la Constitución y que deben garantizarse en los procesos de carácter penal. Más aun, el Estado, al establecer, implementar y aplicar las facultades y procedimientos previstos en esta sección, debe incorporar garantías que “(...) equilibren la aplicación de estos mecanismos con la adecuada protección de los derechos humanos y las libertades”. Todo ello, en el marco de los instrumentos internacionales de derechos humanos y la aplicación del principio de proporcionalidad.
33. Es importante señalar también que el proceso para el juzgamiento de los delitos debe regularse exclusivamente mediante ley. De ahí que, si bien no se verifica contradicción de las normas del Convenio con la Constitución, corresponde a la Asamblea Nacional en el marco de la adecuación normativa, implementar las modificaciones que sean necesarias y acordes a la garantía del debido proceso, del derecho a la defensa en

materia penal y las demás garantías establecidas en la Constitución, para el juzgamiento de los delitos contemplados en el Convenio, así como también la configuración legal debería observar criterios de idoneidad, necesidad y proporcionalidad.

34. Así también, se observa que lo relativo a la jurisdicción establecida en el Convenio no incurre en las prohibiciones establecidas en el artículo 422 de la Constitución pues no cede jurisdicción soberana a instancias de arbitraje internacional, en controversias contractuales o de índole comercial, entre el Estado y personas naturales o jurídicas privadas.

3.2.3 Capítulo III del Convenio

35. El *capítulo III* denominado “[c]ooperación internacional” contiene dos secciones cuyo contenido se sintetiza a continuación:

35.1. La **primera sección denominada** “principios generales” a su vez, se encuentra integrada por cuatro títulos:

35.1.1. El primer título trata sobre “principios generales relativos a la cooperación internacional” que está conformado por el artículo 23 cuyo contenido versa sobre principios generales de cooperación de las partes del Convenio.

35.1.2. El segundo título que refiere a los “principios relativos a la extradición”, integrado por el artículo 24 que a su vez contiene siete numerales, que a efectos del análisis se citan a continuación:

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

35.1.3. El título 3 aborda “los principios relativos a la asistencia mutua” conformado por el artículo 25 que entre otras disposiciones contempla que “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 [...]”. También lo integra el artículo 26 del Convenio que trata sobre la “información espontánea”, en el cual, se contempla que “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 [...]”.

35.1.4. El título 4 trata sobre “[p]rocedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables” y está conformado por el artículo 27 que aborda dicho procedimiento. En su numeral 4 se faculta al Estado requerido a denegar la asistencia solicitada si: “a. la demanda se refiere a una infracción que el Estado requerido considera de naturaleza política o vinculada a una información de naturaleza política o; b. si el Estado requerido estima que, de acceder a la colaboración, se pondría en peligro su soberanía, seguridad, orden público u otro interés esencial”. Con lo cual el Estado parte puede declinar la asistencia si aquella tiene relación con delitos políticos considerados como tales por dicho Estado o por razones de soberanía, seguridad, orden público

u otros “intereses esenciales” del Estado parte. El artículo 28 trata sobre la “confidencialidad y restricciones de uso”.

36. De la revisión de esta sección del Convenio, se observa que el artículo 23 sobre los principios generales de cooperación, el artículo 25 sobre asistencia mutua, el artículo 26 sobre información espontánea y el artículo 27 sobre procedimientos relativos a solicitudes de asistencia mutua si no hay acuerdos internacionales guardan conformidad con los principios de relaciones internacionales contemplados en el artículo 416.1 de la Constitución, en el que Ecuador proclama el principio de cooperación entre Estados, y las normas constitucionales que aseguran el ejercicio de la soberanía del Estado específicamente en relación a los artículos 1 y 3.2 de la Constitución.
37. En cuanto, al artículo 24 del Convenio, este contempla a la extradición entre las Partes por los delitos que se contemplan en este tratado internacional, la cual, debe observar lo dispuesto en el artículo 79 de la Constitución vigente.⁹
38. La **sección 2 titulada** “disposiciones específicas” contiene tres títulos:

38.1.1. El título 1 trata sobre la “asistencia mutua en materia de medidas provisionales”, el cual está conformado por el artículo 29 que aborda la “[c]onservación rápida de datos informáticos almacenados” y que a efectos del análisis de constitucionalidad se cita a continuación:

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;

⁹ En virtud del referéndum realizado el 21 de abril de 2024, se consultó a la ciudadanía sobre la enmienda del artículo 79 de la Constitución, cuyos resultados aún no se han proclamado oficialmente.

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.

38.1.2. En tanto que, el artículo 30 que versa sobre la “[r]evelación rápida de datos conservados”, en los siguientes términos:

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 soberana, seguridad, orden público u otros intereses esenciales.

38.1.3. El título 2 aborda la “asistencia mutua en relación con los poderes de investigación” y está conformado por el artículo 31 que contiene disposiciones específicas sobre este aspecto, el artículo 32 que regula el “Acceso transfronterizo a datos almacenados, con consentimiento o cuando sean accesibles al público”, el artículo 33 sobre “Asistencia mutua para la obtención en tiempo real de datos relativos al tráfico” y el artículo 34 que aborda la “Asistencia mutua en relación con la interceptación de datos relativos al contenido”.

38.1.4. El título 3 se denomina “Red 24/7” y lo integra el artículo 35, en el que entre otros aspectos dispone que: “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”.

39. En cuanto, a los artículos 29 al 35 que están acorde con la obligación del Estado de garantizar “la seguridad integral” de conformidad con el artículo 3.8 de la Constitución, a través de la colaboración internacional y asistencia mutua, así como de regulaciones que permitan la conservación, acceso, recolección, interceptación de la información y designación de un punto de contacto 24/7, responsable de garantizar la asistencia inmediata en investigaciones y procedimientos sobre los ciberdelitos. Los artículos bajo análisis del Convenio se encuentran relacionados con el derecho consagrado en el numeral 66 numeral 21 de la Constitución en el que se reconoce:

el derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación.

40. En este sentido, la Corte verifica que dichos mecanismos de cooperación mutua están restringidos a la existencia de una investigación penal que no están exentos del cumplimiento de los derechos y garantías previstas en los artículos 76 y 77 de la Constitución y que rigen a este tipo de procesos. En consecuencia, los artículos de la sección revisada guardan conformidad con la Constitución, siempre que se observen los derechos que aseguran el debido proceso y defensa en el juzgamiento de estas conductas.

3.2.4 Capítulo IV del Convenio

41. El *capítulo IV* denominada “Cláusulas finales” que contiene aspectos relativos a la firma y entrada en vigor en el artículo 36, la adhesión al convenio en el artículo 37, la aplicación territorial en el artículo 38, los efectos del convenio en el artículo 39, las declaraciones en el artículo 40, la cláusula federal en el artículo 41, las reservas en el artículo 42, el mantenimiento y retirada de las reservas en el artículo 43. El artículo 42 expresamente indica que aquellos artículos sobre los cuales los Estados partes están habilitados a realizar la reserva:

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.

42. De igual manera, el artículo 44 trata sobre la solución de controversias en el artículo 45, las consultas entre las Partes en el artículo 46, denuncia en el artículo 47 y la notificación en el artículo 48. En estos artículos se constata que el Convenio no incurre en las prohibiciones establecidas en el artículo 422 de la Constitución pues no cede jurisdicción soberana a instancias de arbitraje internacional, en controversias contractuales o de índole comercial, entre el Estado y personas naturales o jurídicas privadas.
43. Esta sección refiere al trámite que debe seguirse para la adhesión al Convenio, aspectos que guardan conformidad con lo previsto en los artículos 417 a 422 de la Constitución que regula la suscripción y ratificación de tratados internacionales.

4. Dictamen

En mérito de lo expuesto, administrando justicia constitucional y por mandato de la Constitución de la República del Ecuador, el Pleno de la Corte Constitucional resuelve:

1. *Declarar* la constitucionalidad del “Convenio sobre Ciberdelincuencia”.
2. Disponer que se notifique a la Presidencia de la República el presente dictamen, a fin de que se haga conocer el mismo a la Asamblea Nacional.
3. Notifíquese, publíquese y cúmplase.

ALI VICENTE
LOZADA PRADO

Firmado digitalmente
por ALI VICENTE
LOZADA PRADO

Alí Lozada Prado
PRESIDENTE

Razón: Siento por tal, que el dictamen que antecede fue aprobado por el Pleno de la Corte Constitucional con nueve votos a favor de los Jueces Constitucionales Karla Andrade Quevedo, Alejandra Cárdenas Reyes, Carmen Corral Ponce, Jhoel Escudero Soliz, Enrique Herrería Bonnet, Alí Lozada Prado, Teresa Nuques Martínez, Richard Ortiz Ortiz y Daniela Salazar Marín, en sesión jurisdiccional ordinaria de jueves 25 de abril de 2024.- Lo certifico.

Firmado electrónicamente
Aída García Berni
SECRETARIA GENERAL



Firmado electrónicamente por:
AIDA SOLEDAD GARCIA BERNI



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 incumbran 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 dimanen del presente artículo.

Artículo 47 – Denuncia

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

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

Artículo 48 – Notificación

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

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

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

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

