LEY No. 1928 24 JUL 2018

POR MEDIO DE LA CUAL SE APRUEBA EL «CONVENIO SOBRE LA CIBERDELINCUENCIA», ADOPTADO EL 23 DE NOVIEMBRE DE 2001, EN BUDAPEST

EL CONGRESO DE COLOMBIA

VISTO EL TEXTO DEL **«CONVENIO SOBRE LA CIBERDELINCUENCIA», ADOPTADO EL 23 DE NOVIEMBRE DE 2001, EN BUDAPEST.**

Se adjunta copia fiel y completa del texto certificado en español del Convenio, certificado por la jefe de Área sw la oficina de interpretación de Lenguas del Ministerio de Asuntos Exteriores del Reino de España, certificado por la Coordinadora del Grupo Interno de Trabajo de Tratados de la Direccion de Asuntos Jurídicos Internacionales del Ministerio de Relaciones Exteriores, documento que reposa en el Archivo de del Grupo Interno de Trabajo de Tratados y consta de dieciséis (16) folios.

El presente Proyecto de Ley consta de veinticuatro (24) folios

PROYECTO DE LEY N° 58 | 17

"POR MEDIO DE LA CUAL SE APRUEBA EL *«CONVENIO SOBRE LA CIBERDELINCUENCIA»*, ADOPTADO EL 23 DE NOVIEMBRE DE 2001, EN BUDAPEST."

EL CONGRESO DE LA REPÚBLICA

Visto el texto del *«CONVENIO SOBRE LA CIBERDELINCUENCIA»*, ADOPTADO EL 23 DE NOVIEMBRE DE 2001, EN BUDAPEST.

Se adjunta copia fiel y completa del texto en español del Convenio, certificado por la Jefe de Área de la Oficina de Interpretación de Lenguas del Ministerio de Asuntos Exteriores del Reino de España, certificado por la Coordinadora del Grupo Interno de Trabajo de Tratados de la Dirección de Asuntos Jurídicos Internacionales del Ministerio de Relaciones Exteriores, documento que reposa en el Archivo del Grupo Interno de Trabajo de Tratados y consta en dieciséis (16) folios.

El presente Proyecto de Ley consta de veinticuatro (24) folios.

CONSEJO DE EUROPA

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 conseguir una unión más estrecha entre sus miembros;

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

Convencidos de la necesidad de aplicar, con carácter prioritario, una política penal común encaminada a proteger a la sociedad frente a la ciberdelincuencia, entre otras formas, mediante la adopción de la legislación adecuada y el fomento de la cooperación internacional;

Conscientes de los profundos cambios provocados por la digitalización, la convergencia y la globalización continua 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 una cooperación entre los Estados y el sector privado en la lucha contra la ciberdelincuencia, así como la necesidad de proteger los legítimos intereses en la utilización y el desarrollo de las tecnologías de la información;

En la creencia de que la lucha efectiva contra la ciberdelincuencia requiere una cooperación internacional en materia penal reforzada, rápida y operativa;

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

Conscientes de 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 de 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 de todos a defender sus opiniones sin interferencia alguna, así como la libertad de expresión, que comprende la libertad de buscar, obtener y comunicar información e ideas de todo tipo, sin consideración de fronteras, así como el respeto de la intimidad;

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

Considerando la Convención de las Naciones Unidas sobre los Derechos del Niño (1989) y el Convenio de la Organización Internacional del Trabajo sobre las peores formas de trabajo de los menores (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 presente Convenio pretende completar dichos Convenios con objeto de dotar de mayor eficacia las investigaciones y los procedimientos penales relativos a los delitos relacionados con los sistemas y datos informáticos, así como facilitar la obtención de pruebas electrónicas de los delitos;

Congratulándose de las recientes iniciativas encaminadas a mejorar el entendimiento y la cooperación internacional en la lucha contra la ciberdelincuencia, incluidas las medidas adoptadas 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 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, así como nº R (89) 9 sobre la delincuencia relacionada con la informática, que ofrece directrices a los legisladores nacionales para la definición de determinados delitos informáticos, y nº R (95) 13 relativa a las cuestiones de procedimiento penal vinculadas a la tecnología de la información;

Teniendo en cuenta la Resolución nº 1, adoptada por los Ministros europeos de Justicia en su XXI Conferencia (Praga, 10 y 11 de junio de 1997), que recomendaba al Comité de Ministros apoyar las actividades relativas a la ciberdelincuencia desarrolladas por el Comité Europeo de Problemas Penales (CDPC) para 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 europeos de Justicia (Londres, 8 y 9 de junio de 2000), que animaba a las Partes negociadoras a proseguir sus esfuerzos para encontrar soluciones que permitan que el mayor número posible de Estados pasen a ser Partes en el Convenio, y reconocía la necesidad de un sistema rápido y eficaz de cooperación internacional que refleje debidamente 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), para buscar 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, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa;

b por "datos informáticos" se entenderá cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado 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 por medio de un sistema informático, y

ii cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios de ese servicio;

d por "datos sobre el tráfico" se entenderá cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y 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 la totalidad o a una parte de un sistema informático. Cualquier Parte podrá exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático.

Artículo 3 - Interceptación ilícita

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos. Cualquier Parte podrá exigir que el delito se haya cometido con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

Artículo 4 - Interferencia en los datos

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 actos que dañen, borren, deterioren, alteren o supriman datos informáticos.

2 Cualquier Parte podrá reservarse el derecho a exigir que los actos definidos en el apartado 1 provoquen daños graves.

Artículo 5 - Interferencia en el 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, provocación de daños, 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 un dispositivo, incluido un programa informático, diseñado o adaptado principalmente para la comisión de cualquiera de los delitos previstos de conformidad con los anteriores artículos 2 a 5;

ii una contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático,

con el fin de que sean utilizados para la comisión de cualquiera de los delitos contemplados en los artículos 2 a 5; y

b la posesión de alguno de los elementos contemplados en los anteriores apartados a.i) o ii) con el fin de que sean utilizados para cometer cualquiera de los delitos previstos en los artículos 2 a 5. Cualquier Parte podrá exigir en su derecho interno que se posea un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

2 No podrá interpretarse que el presente artículo impone responsabilidad penal

en los casos en que la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición mencionadas en el apartado 1 del presente artículo no tengan por objeto la comisión de un delito previsto de conformidad con los artículos 2 a 5 del presente Convenio, como es el caso de las pruebas autorizadas o de la protección de un sistema informático.

3 Cualquier Parte podrá reservarse el derecho a no aplicar lo dispuesto en el apartado 1 del presente artículo, siempre que la reserva no afecte a la venta, la distribución o cualquier otra puesta a disposición de los elementos indicados en el apartado 1.a.ii) del presente artículo.

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, cuando se cometa de forma deliberada e ilegítima, la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles. Cualquier Parte podrá exigir que exista una intención fraudulenta o una intención delictiva similar para que se considere que existe responsabilidad penal.

Artículo 8 - Fraude informático

Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante:

a cualquier introducción, alteración, borrado o supresión de datos informáticos;

b cualquier interferencia en el funcionamiento de un sistema informático,

con la intención fraudulenta o delictiva de obtener ilegítimamente 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 vistas a su difusión por medio de un sistema informático;

b la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático;

c la difusión o transmisión de pornografía infantil por medio de un sistema informático,

d la adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona;

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

2 A los efectos del anterior apartado 1, por "pornografía infantil" se entenderá todo material pornográfico que contenga la representación visual de:

a un menor comportándose de una forma sexualmente explícita;

b una persona que parezca un menor comportándose de una forma sexualmente explícita;

c imágenes realistas que representen a un menor comportándose de una forma sexualmente explícita.

3 A los efectos del anterior apartado 2, por "menor" se entenderá toda persona menor de 18 años. No obstante, cualquier Parte podrá establecer un límite de edad inferior, que será como mínimo de 16 años.

4 Cualquier Parte podrá reservarse el derecho a no aplicar, en todo o en parte, las letras d) y e) del apartado 1, y las letras b) y c) del apartado 2.

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, según se definan en la legislación de dicha Parte, de conformidad con las obligaciones asumidas en aplicación del Acta de París de 24 de julio de 1971 por la que se revisó el Convenio de Berna para la

protección de 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 la propiedad intelectual, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando esos 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 la legislación de dicha Parte, de conformidad con las obligaciones que ésta 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 las obras de los intérpretes y ejecutantes y los fonogramas, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

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

Título 5 - Otras formas de responsabilidad y de sanciones

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 intencionada con vistas a la comisión de alguno de los delitos previstos de conformidad con los artículos 2 a 10 del presente Convenio, con la intención de que se cometa ese delito.

2 Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno cualquier tentativa de comisión de alguno de las delitos previstos de conformidad con los artículos 3 a 5, 7, 8, 9.1.a) y c) del presente Convenio, cuando dicha tentativa sea intencionada.

3 Cualquier Estado podrá reservarse el derecho a no aplicar, en todo o en parte, el apartado 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 de conformidad con el presente Convenio, cuando sean cometidos por cuenta de las mismas por cualquier persona física, tanto en calidad individual como en su condición de miembro de un órgano de dicha persona jurídica, que ejerza funciones directivas en la misma, 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 la persona jurídica.

2 Además de los casos ya previstos en el apartado 1 del presente artículo, cada Parte adoptará las medidas necesarias para asegurar que pueda exigirse responsabilidad a una persona jurídica cuando la falta de vigilancia o de control por parte de una persona física mencionada en el apartado 1 haya hecho posible la comisión de un delito previsto de conformidad con el presente Convenio en beneficio de dicha persona jurídica por una persona física que actúe bajo su autoridad.

3 Con sujeción a 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 de conformidad con los artículos 2 a 11 puedan dar lugar a la aplicación de sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad.

2 Cada Parte garantizará la imposición de sanciones o de 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 sobre 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 para los fines de investigaciones o procedimientos penales específicos.

2 Salvo que se establezca específicamente otra cosa en el artículo 21, cada Parte aplicará los poderes y procedimientos mencionados en el apartado 1 del presente artículo a:

a los delitos previstos de conformidad con los artículos 2 a 11 del presente Convenio;

b otros delitos cometidos por medio de un sistema informático; y

c la obtención de pruebas electrónicas de un delito.

3 a Cualquier Parte podrá reservarse el derecho a aplicar las medidas indicadas en el artículo 20 exclusivamente a los delitos o categorías de delitos especificados en la reserva, siempre que el ámbito de dichos delitos o categorías de delitos no sea más reducido que el de los delitos a los que esa Parte aplique las medidas indicadas en el artículo 21. Las Partes procurarán limitar dichas reservas para permitir la aplicación más amplia posible de la medida indicada en el artículo 20.

b Cuando, como consecuencia de las limitaciones existentes en su legislación vigente en el momento de la adopción del presente Convenio, una Parte no pueda aplicar las medidas indicadas en los artículos 20 y 21 a las comunicaciones transmitidas en el sistema informático de un proveedor de servicios:

i utilizado en beneficio de un grupo restringido de usuarios, y

ii que no utilice las redes públicas de comunicaciones ni 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. Cada Parte procurará limitar este tipo de reservas de forma que se permita la aplicación más amplia posible de las medidas indicadas en los artículos 20 y 21.

Artículo 15 - Condiciones y salvaguardas

1 Cada Parte se asegurará de que el establecimiento, la ejecución y la aplicación

de los poderes y procedimientos previstos en la presente sección están sujetas a las condiciones y salvaguardas previstas en su derecho interno, que deberá garantizar una protección adecuada de los derechos humanos y de las libertades, incluidos los derechos derivados de las obligaciones asumidas en virtud del Convenio del Consejo de Europa para la protección de los derechos humanos y las libertades fundamentales (1950), del Pacto Internacional de derechos civiles y políticos de las Naciones Unidas (1966), y de otros instrumentos internacionales aplicables en materia de derechos humanos, y que deberá integrar el principio de proporcionalidad.

2 Cuando resulte procedente dada la naturaleza del procedimiento o del poder de que se trate, dichas condiciones incluirán, entre otros aspectos, la supervisión judicial u otra forma de supervisión independiente, los motivos que justifiquen la aplicación, y la limitación del ámbito de aplicación y de la duración del poder o del procedimiento de que se trate.

3 Siempre que sea conforme con el interés público y, en particular, con la correcta administración de la justicia, cada Parte examinará la repercusión de los poderes y procedimientos previstos en la presente sección en 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 otra manera la conservación rápida de determinados datos electrónicos, incluidos los datos sobre el tráfico, almacenados por medio de un sistema informático, en particular cuando existan razones para creer que los datos informáticos resultan especialmente susceptibles de pérdida o de modificación.

2 Cuando una Parte aplique lo dispuesto en el anterior apartado 1 por medio de una orden impartida a una persona para conservar determinados datos almacenados que se encuentren en posesión o bajo el control de dicha persona, la Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar a esa persona a conservar y a proteger la integridad de dichos datos durante el tiempo necesario, hasta un máximo de noventa días, de manera que las autoridades competentes puedan conseguir su revelación. Las Partes podrán prever que tales órdenes sean renovables.

3 Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para obligar al encargado de la custodia de los datos o a otra persona encargada de su conservación a mantener en secreto la aplicación de

dichos procedimientos durante el plazo 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 datos sobre el tráfico

1 Para garantizar la conservación de los datos sobre el tráfico en aplicación de lo dispuesto en el artículo 16, cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias:

a para asegurar la posibilidad de conservar rápidamente dichos datos sobre el tráfico con independencia de que en la transmisión de esa comunicación participaran uno o varios proveedores de servicios, y

b para garantizar la revelación rápida a la autoridad competente de la Parte, o a una persona designada por dicha autoridad, de un volumen suficiente de datos sobre el tráfico para que dicha Parte pueda identificar a los proveedores de servicio y la vía por la que se transmitió la comunicación.

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 que se encuentre en su territorio que comunique determinados datos informáticos que posea o que se encuentren bajo su control, almacenados en un sistema informático o en un medio de almacenamiento de datos informáticos; y

b a un proveedor de servicios que ofrezca prestaciones en el territorio de esa Parte que comunique los datos que posea o que se encuentren bajo su control relativos a los abonados en conexión con dichos servicios.

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

3 A los efectos del presente artículo, por "datos relativos a los abonados" se entenderá toda información, en forma de datos informáticos o de cualquier otra

forma, que posea un proveedor de servicios y esté relacionada con los abonados a dichos servicios, excluidos los datos sobre el tráfico o sobre el contenido, y que permita determinar:

a el tipo de servicio de comunicaciones utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio;

b la identidad, la dirección postal o geográfica y el número de teléfono del abonado, así como cualquier otro número de acceso o información sobre facturación y pago que se encuentre disponible sobre la base de un contrato o de un acuerdo de prestación de servicios;

c cualquier otra información relativa al lugar en que se encuentren los equipos de comunicaciones, disponible sobre la base de un contrato o de un acuerdo de servicios.

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 una forma similar:

a a un sistema informático o a una parte del mismo, así como a los datos informáticos almacenados en el mismo; y

b a un medio de almacenamiento de datos informáticos en el que puedan almacenarse datos informáticos,

en su territorio.

2 Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para asegurar que, cuando sus autoridades procedan al registro o tengan acceso de una forma similar a un sistema informático específico o a una parte del mismo, de conformidad con lo dispuesto en el apartado 1.a, y tengan razones para creer que los datos buscados están almacenados en otro sistema informático o en una parte del mismo situado en su territorio, y dichos datos sean lícitamente accesibles a través del sistema inicial o estén disponibles para éste, dichas autoridades puedan ampliar rápidamente el registro o la forma de acceso 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 una forma similar los datos informáticos a los que se haya tenido acceso en

aplicación de lo dispuesto en los apartados 1 ó 2. Estas medidas incluirán las siguientes facultades:

a confiscar u obtener de una forma similar un sistema informático o una parte del mismo, o un medio de almacenamiento de datos informáticos;

b realizar y conservar una copia de dichos datos informáticos;

c preservar la integridad de los datos informáticos almacenados de que se trate;

d hacer inaccesibles o suprimir dichos datos informáticos del sistema informático al que se ha tenido acceso.

4 Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite toda la información necesaria, dentro de lo razonable, para permitir la aplicación de las medidas indicadas en los apartados 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 sobre el 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 mediante la aplicación de medios técnicos existentes en su territorio, y

b obligar a un proveedor de servicios, dentro de los límites de su capacidad técnica:

i a obtener o grabar mediante la aplicación de medios técnicos existentes en su territorio, o

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

en tiempo real los datos sobre el tráfico asociados a comunicaciones específicas transmitidas en su territorio por medio de un sistema

informático.

2 Cuando una Parte, en virtud de los principios consagrados en su ordenamiento jurídico interno, no pueda adoptar las medidas indicadas en el apartado 1.a), podrá adoptar en su lugar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos sobre el tráfico asociados a determinadas comunicaciones transmitidas en su territorio mediante la aplicación de los medios técnicos existentes en el mismo.

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 ha 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 sobre el contenido

1 Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para facultar a las autoridades competentes, por lo que respecta a una serie de delitos graves que deberán definirse en su derecho interno:

a a obtener o a grabar mediante la aplicación de medios técnicos existentes en su territorio, y

b a obligar a un proveedor de servicios, dentro de los límites de su capacidad técnica:

i a obtener o a grabar mediante la aplicación de los medios técnicos existentes en su territorio, o

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

en tiempo real los datos sobre el contenido de determinadas comunicaciones en su territorio, transmitidas por medio de un sistema informático.

2 Cuando una Parte, en virtud de los principios consagrados en su ordenamiento jurídico interno, no pueda adoptar las medidas indicadas en el apartado 1.a), podrá adoptar en su lugar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos sobre el contenido de determinadas comunicaciones transmitidas en su territorio mediante la aplicación de los medios técnicos existentes en el mismo.

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 ha 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 con arreglo a los artículos 2 a 11 del presente Convenio, siempre que se haya cometido:

a en su territorio; o

b a bordo de un buque que enarbole pabellón de dicha Parte; o

c a bordo de una aeronave matriculada según las leyes de dicha Parte; 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 Cualquier Estado podrá reservarse el derecho a no aplicar o a aplicar únicamente en determinados casos o condiciones las normas sobre jurisdicción establecidas en los apartados 1.b) a 1.d) del presente artículo o en cualquier otra parte de los mismos.

3 Cada Parte adoptará las medidas que resulten necesarias para afirmar su jurisdicción respecto de los delitos mencionados en el apartado 1 del artículo 24 del presente Convenio, cuando el presunto autor del delito se encuentre en su territorio y no pueda ser extraditado a otra Parte por razón de su nacionalidad, previa solicitud de extradición.

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

5 Cuando varias Partes reivindiquen su jurisdicción respecto de un presunto delito contemplado en el presente Convenio, las Partes interesadas celebrarán consultas, siempre que sea oportuno, con miras a determinar cuál es la jurisdicción más adecuada para las actuaciones penales.

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 aplicables a la cooperación internacional en materia penal, de acuerdos basados en legislación uniforme o recíproca y de su derecho interno, para los fines de las investigaciones o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para la obtención de pruebas electrónicas 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 establecidos en los artículos 2 a 11 del presente Convenio, siempre que estén castigados en la legislación de las dos Partes implicadas con una pena privativa de libertad de una duración máxima de como mínimo un año, o con una pena más grave.

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

2 Se considerará que los delitos mencionados en el apartado 1 del presente artículo están incluidos entre los delitos que dan lugar a extradición en cualquier tratado de extradición vigente entre las Partes. Las Partes se comprometen a incluir dichos delitos entre los que pueden dar lugar a extradición en cualquier tratado de extradición que puedan celebrar entre sí.

3 Cuando una Parte que condicione la extradición a la existencia de un tratado reciba una solicitud de extradición de otra Parte con la que no haya celebrado ningún tratado de extradición, podrá aplicar el presente Convenio como fundamento jurídico de la extradición respecto de cualquier delito mencionado en el apartado 1 del presente artículo.

4 Las Partes que no condicionen la extradición a la existencia de un tratado

reconocerán los delitos mencionados en el apartado 1 del presente artículo como delitos que pueden dar lugar a extradición entre ellas.

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

6 Cuando se deniegue la extradición por un delito mencionado en el apartado 1 del presente artículo únicamente por razón de la nacionalidad de la persona buscada 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 para los fines de las actuaciones penales pertinentes, e informará a su debido tiempo del resultado final a la Parte requirente. Dichas autoridades tomarán su decisión y efectuarán sus investigaciones y procedimientos de la misma manera 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 solicitudes de extradición o de detención provisional en ausencia de un 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 concederán asistencia mutua en la mayor medida posible para los fines de las investigaciones o procedimientos relativos a delitos relacionados con sistemas y datos informáticos o para la obtención de pruebas en formato electrónico de un delito.

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

3 En casos de urgencia, cada Parte podrá transmitir solicitudes de asistencia o comunicaciones relacionadas con las mismas por medios rápidos de comunicación, incluidos el fax y el correo electrónico, en la medida en que

dichos medios ofrezcan niveles adecuados de seguridad y autenticación (incluido el cifrado, en caso necesario), con confirmación oficial posterior si la Parte requerida lo exige. La Parte requerida aceptará la solicitud y dará respuesta a la misma por cualquiera de estos medios rápidos de comunicación.

4 Salvo que se establezca específicamente otra cosa en los artículos del presente capítulo, la asistencia mutua estará sujeta a las condiciones previstas en el derecho interno de la Parte requerida o en los tratados de asistencia mutua aplicables, incluidos los motivos por los que la Parte requerida puede denegar la cooperación. La Parte requerida no ejercerá el derecho a denegar la asistencia mutua en relación con los delitos mencionados en los artículos 2 a 11 únicamente porque la solicitud se refiere a un delito que considera de naturaleza fiscal.

5 Cuando, de conformidad con las disposiciones del presente capítulo, se permita a la Parte requerida condicionar la asistencia mutua a la existencia de una doble tipificación penal, dicha condición se considerará cumplida cuando la conducta constitutiva del delito respecto del cual se solicita la asistencia constituya un delito en virtud de su derecho interno, con independencia de que dicho derecho incluya o no el delito dentro de la misma categoría de delitos 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 petición previa, una Parte podrá comunicar a otra Parte información obtenida en el marco de sus propias investigaciones cuando considere que la revelación de dicha información podría ayudar a la Parte receptora a iniciar o llevar a cabo investigaciones o procedimientos en relación con delitos previstos en el presente Convenio o podría dar lugar a una petición de cooperación de dicha Parte en virtud del presente capítulo.

2 Antes de comunicar dicha información, la Parte que la comunique podrá solicitar que se preserve su confidencialidad o que se utilice con sujeción a determinadas condiciones. Si la Parte receptora no puede atender esa solicitud, informará de ello a la otra Parte, que deberá entonces determinar si a pesar de ello debe facilitarse la información o no. Si la Parte destinataria acepta la información en las condiciones establecidas, quedará vinculada por las mismas.

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 Cuando entre las Partes requirente y requerida no se encuentre vigente un tratado de asistencia mutua o un acuerdo basado en legislación uniforme o recíproca, serán de aplicación las disposiciones de los apartados 2 a 10 del presente artículo. Las disposiciones del presente artículo no serán de aplicación cuando exista un tratado, acuerdo o legislación de este tipo, salvo que las Partes interesadas convengan en 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 solicitudes de asistencia mutua y de dar respuesta a las mismas, de su ejecución y de su remisión a las autoridades competentes para su ejecución.

b Las autoridades centrales se 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 cumplimiento del presente apartado.

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 los procedimientos especificados por la Parte requirente, salvo que sean incompatibles con la legislación de la Parte requerida.

4 Además de las condiciones o de los motivos de denegación contemplados en el apartado 4 del artículo 25, la Parte requerida podrá denegar la asistencia si:

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

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

5 La Parte requerida podrá posponer su actuación en respuesta a una solicitud cuando dicha actuación pudiera causar perjuicios a investigaciones o procedimientos llevados a cabo por sus autoridades.

6 Antes de denegar o posponer la asistencia, la Parte requerida estudiará, previa consulta cuando proceda con la Parte requirente, si puede atenderse la solicitud parcialmente o con sujeción a las condiciones que considere necesarias.

7 La Parte requerida informará sin demora a la Parte requirente del resultado de la ejecución de una solicitud de asistencia. Deberá motivarse cualquier denegación o aplazamiento de la asistencia solicitada. La Parte requerida informará también a la Parte requirente de cualquier motivo que haga imposible la ejecución de la solicitud o que pueda retrasarla de forma significativa.

8 La Parte requirente podrá solicitar a la Parte requerida que preserve la confidencialidad de la presentación de una solicitud en virtud del presente capítulo y del objeto de la misma, salvo en la medida necesaria para su ejecución. Si la Parte requerida no puede cumplir esta petición de confidencialidad, lo comunicará inmediatamente a la Parte requirente, que determinará entonces si pese a ello debe procederse a la ejecución de la solicitud.

9 a En casos de urgencia, las solicitudes de asistencia mutua o las comunicaciones al respecto podrán ser enviadas directamente por las autoridades judiciales de la Parte requirente a las autoridades correspondientes de la Parte requerida. En tal caso, se enviará al mismo tiempo copia a la autoridad central de la Parte requerida a través de la autoridad central de la Parte requirente.

b Cualquier solicitud o comunicación en virtud de este apartado podrá efectuarse a través de la Organización Internacional de Policía Criminal (INTERPOL).

c Cuando se presente una solicitud en aplicación de la letra a) del presente artículo y la autoridad no sea competente para tramitarla, remitirá la solicitud a la autoridad nacional competente e informará directamente a la Parte requirente de dicha remisión.

d Las solicitudes y comunicaciones efectuadas en virtud del presente apartado que no impliquen medidas coercitivas podrán ser remitidas 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 el depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, cada Parte podrá informar al Secretario General del Consejo de Europa de que, por razones de eficacia, las solicitudes formuladas en virtud del presente apartado deberán dirigirse a su autoridad central.

Artículo 28 - Confidencialidad y restricción de la utilización

1 En ausencia de un tratado de asistencia mutua o de un acuerdo basado en legislación uniforme o recíproca que esté vigente entre las Partes requirente y

requerida, serán de aplicación las disposiciones del presente artículo. Las disposiciones del presente artículo no serán de aplicación cuando exista un tratado, acuerdo o legislación de este tipo, salvo que las Partes interesadas convengan en aplicar en su lugar la totalidad o una parte del resto del presente artículo.

2 La Parte requerida podrá supeditar la entrega de información o material en respuesta a una solicitud a la condición de que:

a se preserve su confidencialidad cuando la solicitud de asistencia judicial mutua no pueda ser atendida en ausencia de esta condición, o

b no se utilicen para investigaciones o procedimientos distintos de los indicados en la solicitud.

3 Si la Parte requirente no puede cumplir alguna condición de las mencionadas en el apartado 2, informará de ello sin demora a la otra Parte, que determinará en tal caso si pese a ello debe facilitarse la información. Cuando la Parte requirente acepte la condición, quedará vinculada por ella.

4 Cualquier Parte que facilite información o material con sujeción a una condición con arreglo a lo dispuesto en el apartado 2 podrá requerir a la otra Parte que explique, en relación con dicha condición, el uso dado a dicha información o material.

*Sección 2 - **Disposiciones especiales***

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 asegure de otra forma la conservación rápida de datos almacenados por medio de un sistema informático que se encuentre en el territorio de esa otra Parte, respecto de los cuales la Parte requirente tenga la intención de presentar una solicitud de asistencia mutua con vistas al registro o al acceso de forma similar, la confiscación o la obtención de forma similar, o la revelación de los datos.

2 En las solicitudes de conservación que se formulen en virtud del apartado 1 se indicará:

a la autoridad que solicita dicha conservación;

b el delito objeto de investigación o de procedimiento penal y un breve resumen de los hechos relacionados con el mismo;

c los datos informáticos almacenados que deben conservarse y su relación con el delito;

d cualquier información disponible que permita identificar a la persona encargada de la custodia de los datos informáticos almacenados o la ubicación del sistema informático;

e la necesidad de la conservación; y

f que la Parte tiene la intención de presentar una solicitud de asistencia mutua para el registro o el acceso de forma similar, la confiscación o la obtención de forma similar o la revelación de los datos informáticos almacenados.

3 Tras recibir la solicitud de otra Parte, la Parte requerida tomará las medidas adecuadas para conservar rápidamente los datos especificados de conformidad con su derecho interno. A los efectos de responder a una solicitud, no se requerirá la doble tipificación penal como condición para proceder a la conservación.

4 Cuando una Parte exija la doble tipificación penal como condición para atender una solicitud de asistencia mutua para el registro o el acceso de forma similar, la confiscación o la obtención de forma similar o la revelación de datos almacenados, dicha Parte podrá reservarse, en relación con delitos distintos de los previstos con arreglo a los artículos 2 a 11 del presente Convenio, el derecho a denegar la solicitud de conservación en virtud del presente artículo en los casos en que tenga motivos para creer que la condición de la doble tipificación penal no podrá cumplirse en el momento de la revelación.

5 Asimismo, las solicitudes de conservación únicamente podrán denegarse si:

a la solicitud hace referencia a un delito que la Parte requerida considera delito político o delito relacionado con un delito político;

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 no bastará para garantizar la futura disponibilidad de los datos o pondrá en peligro la confidencialidad de la investigación de la Parte requirente o causará cualquier otro perjuicio a la misma, informará de ello sin demora a la Parte requirente, la cual decidirá entonces si debe pese a ello procederse a la ejecución de la solicitud.

7 Las medidas de conservación adoptadas en respuesta a la solicitud mencionada en el apartado 1 tendrán una duración mínima de sesenta días, con objeto de permitir a la Parte requirente presentar una solicitud de registro o de acceso de forma similar, confiscación u obtención de forma similar, o de revelación de los datos. Cuando se reciba dicha solicitud, seguirán conservándose los datos hasta que se adopte una decisión sobre la misma.

Artículo 30 - Revelación rápida de datos conservados sobre el tráfico

1 Cuando, con motivo de la ejecución de una solicitud presentada de conformidad con el artículo 29 para la conservación de datos sobre el tráfico en relación con una comunicación específica, la Parte requerida descubra que un proveedor de servicios de otro Estado participó en la transmisión de la comunicación, la Parte requerida revelará rápidamente a la Parte requirente un volumen suficiente de datos sobre el tráfico para identificar al proveedor de servicios y la vía por la que se transmitió la comunicación.

2 La revelación de datos sobre el tráfico en virtud del apartado 1 únicamente podrá denegarse si:

a la solicitud hace referencia a un delito que la Parte requerida considera delito político o delito relacionado con un delito político;

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 informáticos almacenados

1 Una Parte podrá solicitar a otra Parte que registre o acceda de forma similar, confisque u obtenga de forma similar y revele datos almacenados por medio de un sistema informático situado en el territorio de la Parte requerida, incluidos los datos conservados en aplicación del artículo 29.

2 La Parte requerida dará respuesta a la solicitud aplicando los instrumentos internacionales, acuerdos y legislación mencionados en el artículo 23, así como de conformidad con otras disposiciones aplicables en el presente capítulo.

3 Se dará respuesta lo antes posible a la solicitud cuando:

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

b los instrumentos, acuerdos o legislación mencionados en el apartado 2 prevean la cooperación rápida.

Artículo 32 - Acceso transfronterizo a datos almacenados, con consentimiento o cuando estén a disposición del público

Una Parte podrá, sin la autorización de otra Parte:

a tener acceso a datos informáticos almacenados que se encuentren a disposición del público (fuente abierta), con independencia de la ubicación geográfica de dichos datos; o

b tener acceso o recibir, a través de un sistema informático situado en su territorio, datos informáticos almacenados situados en otra Parte, si la Parte obtiene el consentimiento lícito y voluntario de la persona legalmente autorizada para revelar los datos a la Parte por medio de ese sistema informático.

Artículo 33 - Asistencia mutua para la obtención en tiempo real de datos sobre el tráfico

1 Las Partes se prestarán asistencia mutua para la obtención en tiempo real de datos sobre el tráfico asociados a comunicaciones específicas en su territorio transmitidas por medio de un sistema informático. Con sujeción a lo dispuesto en el apartado 2, dicha asistencia se regirá por las condiciones y procedimientos establecidos en el derecho interno.

2 Cada Parte prestará dicha asistencia como mínimo respecto de los delitos por los que se podría conseguir la obtención en tiempo real de datos sobre el tráfico en un caso similar en su país.

Artículo 34 - Asistencia mutua relativa a la interceptación de datos sobre el contenido

Las Partes se prestarán asistencia mutua para la obtención o grabación en tiempo real de datos sobre el contenido de comunicaciones específicas transmitidas por medio de un sistema informático en la medida en que lo permitan sus tratados y el derecho interno aplicables.

Título 3 - Red 24/7

Artículo 35 - Red 24/7

1 Cada Parte designará un punto de contacto disponible las veinticuatro horas del

día, siete días a la semana, con objeto de garantizar la prestación de ayuda inmediata para los fines de las investigaciones o procedimientos relacionados con delitos vinculados a sistemas y datos informáticos, o para la obtención de pruebas electrónicas de un delito. Dicha asistencia incluirá los actos tendentes a facilitar las siguientes medidas o su adopción directa, cuando lo permitan la legislación y la práctica internas:

a el asesoramiento técnico;

b la conservación de datos en aplicación de los artículos 29 y 30;

c la obtención de pruebas, el suministro de información jurídica y la localización de sospechosos.

2 a El punto de contacto de una Parte estará capacitado para mantener comunicaciones con el punto de contacto de otra Parte con carácter urgente.

b Si el punto de contacto designado por una Parte no depende de la autoridad o de las autoridades de dicha Parte responsables de la asistencia mutua internacional o de la extradición, el punto de contacto velará por garantizar la coordinación con dicha autoridad o autoridades con carácter urgente.

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

Capítulo IV - Disposiciones finales

Artículo 36 - Firma y entrada en vigor

1 El presente Convenio estará 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 tres como mínimo sean Estados miembros del Consejo de Europa, hayan expresado su consentimiento para quedar vinculados por el Convenio de conformidad con lo dispuesto en los apartados 1 y 2.

4 Respecto de cualquier Estado signatario que exprese más adelante 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 su consentimiento para quedar vinculado por el Convenio de conformidad con lo dispuesto en los apartados 1 y 2.

Artículo 37 - Adhesión al Convenio

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

2 Para todo Estado que se adhiera al Convenio de conformidad con lo dispuesto en el anterior apartado 1, 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 de su instrumento de ratificación, aceptación, aprobación o adhesión, cada Estado podrá especificar el territorio o territorios a los que se aplicará el presente Convenio.

2 En cualquier momento posterior, mediante declaración dirigida al Secretario General del Consejo de Europa, cualquier Parte podrá hacer extensiva la aplicación del presente Convenio a cualquier otro territorio especificado en la declaración. Respecto de dicho territorio, el Convenio entrará en vigor 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 apartados anteriores podrá retirarse, 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 dicha notificación.

Artículo 39 - Efectos del Convenio

1 La finalidad del presente Convenio es completar los tratados o acuerdos

multilaterales o bilaterales aplicables entre las Partes, incluidas las disposiciones de:

- el Convenio europeo de extradición, abierto a la firma en París el 13 de diciembre de 1957 (STE nº 24);
- el Convenio europeo de asistencia judicial en materia penal, abierto a la firma en Estrasburgo el 20 de abril de 1959 (STE nº 30);
- el Protocolo adicional al Convenio europeo de asistencia judicial en materia penal, abierto a la firma en Estrasburgo el 17 de marzo de 1978 (STE nº 99).

2 Si dos o más Partes han celebrado ya un acuerdo o tratado sobre las materias reguladas en el presente Convenio o han regulado de otra forma sus relaciones al respecto, o si lo hacen en el futuro, tendrán derecho a aplicar, en lugar del presente Convenio, dicho acuerdo o tratado o a regular dichas relaciones en consonancia. No obstante, cuando las Partes regulen sus relaciones respecto de las materias contempladas en el presente Convenio de forma distinta a la establecida en el mismo, deberán hacerlo de una forma 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 las Partes.

Artículo 40 - Declaraciones

Mediante notificación 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 elementos complementarios según lo dispuesto en los artículos 2, 3, 6.1.b), 7, 9.3 y 27.9.e).

Artículo 41 - Cláusula federal

1 Los Estados federales podrán reservarse el derecho a asumir las obligaciones derivadas del capítulo II del presente Convenio de forma compatible con los principios fundamentales por los que se rija la relación entre su gobierno central y los estados que lo formen u otras entidades territoriales análogas, siempre que siga estando en condiciones de cooperar de conformidad con el capítulo III.

2 Cuando formule una reserva en aplicación del apartado 1, un Estado federal no podrá aplicar los términos de dicha reserva para excluir o reducir sustancialmente sus obligaciones en relación con las medidas contempladas en

el capítulo II. En todo caso, deberá dotarse de una capacidad amplia y efectiva que permita la aplicación de las medidas previstas en dicho capítulo.

3 Por lo que respecta a las disposiciones del presente Convenio cuya aplicación sea competencia de los estados federados o de otras entidades territoriales análogas que no estén obligados por el sistema constitucional de la federación a la adopción de medidas legislativas, el gobierno federal informará de esas disposiciones a las autoridades competentes de dichos estados, junto con su opinión favorable, alentándoles a adoptar las medidas adecuadas para su aplicación.

Artículo 42 - Reservas

Mediante notificación 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 una o varias de las reservas previstas en el apartado 2 del artículo 4, apartado 3 del artículo 6, apartado 4 del artículo 9, apartado 3 del artículo 10, apartado 3 del artículo 11, apartado 3 del artículo 14, apartado 2 del artículo 22, apartado 4 del artículo 29 y apartado 1 del artículo 41. No podrán formularse otras reservas.

Artículo 43 - Situación de las reservas y retirada de las mismas

1 La Parte que haya formulado una reserva de conformidad con el artículo 42 podrá retirarla en todo o en parte mediante notificación 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 que la retirada de una reserva surtirá efecto en una fecha especificada en la misma y ésta es posterior a la fecha en que el Secretario General reciba la notificación, la retirada surtirá efecto en dicha fecha posterior.

2 La Parte que haya formulado una reserva según lo dispuesto en el artículo 42 retirará dicha reserva, en todo o en parte, tan pronto como lo permitan las circunstancias.

3 El Secretario General del Consejo de Europa podrá preguntar periódicamente a las Partes que hayan formulado una o varias reservas según lo dispuesto en el artículo 42 acerca de las perspectivas de que se retire dicha reserva.

Artículo 44 - Enmiendas

1 Cualquier Estado Parte podrá proponer enmiendas al presente Convenio, que serán comunicadas por el Secretario General del Consejo de Europa 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 al presente Convenio o que haya sido invitado a

adherirse al mismo de conformidad con lo dispuesto en el artículo 37.

2 Las enmiendas propuestas por una Parte serán comunicadas al Comité Europeo de Problemas Penales (CDPC), que presentará 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 Partes no miembros en el presente Convenio, podrá adoptar la enmienda.

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

5 Cualquier enmienda adoptada de conformidad con el apartado 3 del presente artículo entrará en vigor treinta días después de que las Partes hayan comunicado su aceptación de la misma al Secretario General.

Artículo 45 - Solución de controversias

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

2 En caso de controversia entre las Partes sobre la interpretación o aplicación del presente Convenio, éstas intentarán resolver la controversia mediante negociaciones 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 o a la Corte Internacional de Justicia, según acuerden las Partes interesadas.

Artículo 46 - Consultas entre las Partes

1 Las Partes se consultarán periódicamente, según sea necesario, con objeto de facilitar:

a la utilización y la aplicación efectivas del presente Convenio, incluida la detección de cualquier problema derivado del mismo, así como los efectos de cualquier declaración o reserva formulada de conformidad con el presente Convenio;

b el intercambio de información sobre novedades significativas de carácter jurídico, político o tecnológico relacionadas con la ciberdelincuencia y con la obtención de pruebas en formato electrónico;

c el estudio de la conveniencia de ampliar o enmendar el presente

Convenio.

2 Se mantendrá periódicamente informado al Comité Europeo de Problemas Penales (CDPC) acerca del resultado de las consultas mencionadas en el apartado 1.

3 Cuando proceda, el CDPC facilitará las consultas mencionadas en el apartado 1 y tomará las medidas necesarias para ayudar a las Partes en sus esfuerzos por ampliar o enmendar el Convenio. Como máximo tres años después de la entrada en vigor del presente Convenio, el Comité Europeo de Problemas Penales (CDPC) llevará a cabo, en cooperación con las Partes, una revisión de todas las disposiciones del Convenio y, en caso necesario, recomendará las enmiendas procedentes.

4 Salvo en los casos en que sean asumidos por el Consejo de Europa, los gastos realizados para aplicar lo dispuesto en el apartado 1 serán sufragados por las Partes en la forma que éstas determinen.

5 Las Partes contarán con la asistencia de la Secretaría del Consejo de Europa para desempeñar sus funciones en aplicación del presente artículo.

Artículo 47 - Denuncia

1 Cualquier Parte podrá 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 y a cualquier Estado que se haya adherido al mismo o que haya sido invitado a hacerlo:

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 formulada en virtud del artículo 40 o reserva formulada

de conformidad con el artículo 42;

e cualquier otro acto, notificación o comunicación relativo al presente Convenio.

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

Hecho en Budapest, el 23 de noviembre de 2001, en francés e inglés, siendo ambos textos igualmente auténticos, en un ejemplar único que se depositará en los archivos del Consejo de Europa. El Secretario General del Consejo de Europa remitirá copias certificadas a cada uno de 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 invitado a adherirse al mismo.

LA JEFE DE ÁREA DE LA OFICINA DE INTERPRETACIÓN DE LENGUAS CERTIFICA: Que la precedente traducción está fiel y literalmente hecha de un documento en francés e inglés que a tal efecto se me ha exhibido. Madrid, a 9 de enero de dos mil dos

LA SUSCRITA COORDINADORA DEL GRUPO INTERNO DE TRABAJO DE TRATADOS DE LA DIRECCIÓN DE ASUNTOS JURÍDICOS INTERNACIONALES DEL MINISTERIO DE RELACIONES EXTERIORES DE LA REPÚBLICA DE COLOMBIA

CERTIFICA:

Que la reproducción del texto que antecede es copia fiel y completa de la copia certificada del *«Convenio sobre la Ciberdelincuencia»*, adoptado el 23 de noviembre de 2001, en Budapest, documento que reposa en los archivos del Grupo Interno de Trabajo de Tratados de la Dirección de Asuntos Jurídicos Internacionales de este Ministerio y que consta en dieciséis (16) folios.

Dada en Bogotá, D.C., a los veintiséis (26) días del mes de mayo de dos mil diecisiete (2017).

OLGA LUCÍA ARENAS NEIRA
Coordinadora del Grupo Interno de Trabajo de Tratados

EXPOSICIÓN DE MOTIVOS DEL PROYECTO DE LEY, POR MEDIO DEL CUAL SE APRUEBA EL *«CONVENIO SOBRE LA CIBERDELINCUENCIA»*, ADOPTADO EL 23 DE NOVIEMBRE DE 2001, EN BUDAPEST

Honorables Senadores y Representantes:

En nombre del Gobierno Nacional, y en cumplimiento del numeral 16 del artículo 150, numeral 2 del artículo 189 y el artículo 224 de la Constitución Política, presentamos a consideración del Honorable Congreso de la República, el Proyecto de Ley por medio de la cual se aprueba el *«Convenio sobre la Ciberdelincuencia»*, adoptado el 23 de noviembre de 2001, en Budapest.

I. CONSIDERACIONES PREVIAS

A. Contexto Internacional

El crecimiento de las amenazas en el ciberespacio, así como la utilización de nuevas tecnologías para generar amenazas informáticas, constituyen una preocupación común, dado que impactan de manera significativa la seguridad de la información, en los ámbitos tanto público como privado. Esto lo que pone de manifiesto es la necesidad de desarrollar de forma estricta políticas de seguridad necesarias para establecer controles que permitan proteger tanto a la ciudadanía sociedad, como al el Estado y sus infraestructuras críticas, ante estas nuevas amenazas. Tales políticas de seguridad han de ser respaldadas por un adecuado marco normativo sustancial y procesal de naturaleza penal, para que su implementación sea efectiva.

Por esta razón, en noviembre de 2001, producto de una reunión internacional de expertos celebrada en Budapest, Hungría, se creó el único marco existente para aplicar una política penal común para proteger a la sociedad frente a la ciberdelincuencia, mediante la adopción de legislación adecuada y el fortalecimiento de la cooperación internacional. En la actualidad, este documento es considerado como el estándar mundial en esta materia.

Varios Estado europeos, junto a otras naciones como Estados Unidos, Japón, Canadá y Sudáfrica, vieron con interés el contenido del Convenio en virtud de que representaba una oportunidad valiosa para contar con un instrumento aplicable en todos los países del mundo y así lograr consenso internacional en la persecución de las nuevas formas de delincuencia ejecutadas a través de los medios telemáticos, considerando que más que cualquier otro fenómeno criminal, la ciberdelincuencia no tiene fronteras.

En la actualidad, el Convenio de Budapest ha sido firmado por 45 de los 47 Estados miembros del Consejo de Europa. De ese grupo, 35 lo han ratificado. Estados no miembros del Consejo de Europa, como Australia, Estados Unidos, Japón, la Isla Mauricio, República Dominicana y Panamá, son Estados Parte del Convenio. Además, más de 24 países han sido invitados a adherirse al Convenio, por lo que en el momento se encuentran adelantando el proceso de ratificación interna en este sentido.

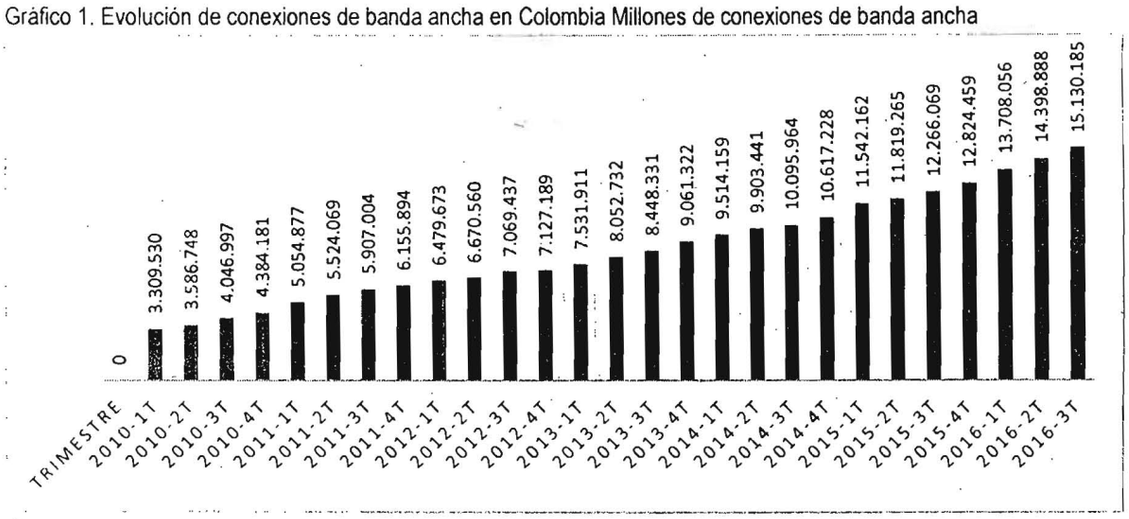
Por su parte, el 11 de septiembre de 2013, Colombia fue invitada por el Consejo de Europa a adherirse al Convenio de Budapest, gracias a las gestiones del Gobierno Nacional encaminadas a contar con instrumentos jurídicos y de cooperación internacional para enfrentar de forma efectiva el delito cibernético. El término establecido para formalizar la adhesión es de 5 años por lo que solo hasta el año 2018 Colombia tiene la posibilidad de aceptar dicha invitación.

B. Contexto Nacional

Colombia es el primer país de América Latina con Internet de alta velocidad que ha tenido como finalidad llevar este medio a todos sus ciudadanos a lo largo del territorio nacional. En el mismo sentido, aproximadamente desde el año 2005, Colombia se ha comprometido a fortalecer la seguridad de la información y desde 2010, cuando se implementó el Plan Vive Digital, el país ha experimentado una revolución digital que ha llevado el uso de las tecnologías de la información y las comunicaciones a ser una herramienta para el desarrollo del país.

Esta revolución digital implica que tanto los ciudadanos como el sector privado y las entidades públicas dependan cada día más de las tecnologías de la información y las comunicaciones, como lo evidencian las últimas cifras registradas, incluyendo las de conexiones de banda ancha en el país, las cuales se multiplicaron significativamente en los últimos años, pasando de 213 millones en 2010, a 15,130 millones en 2016, tal y como se ilustra en el Gráfico 1.

Gráfico 1. Evolución de conexiones de banda ancha en Colombia Millones de conexiones de banda ancha



Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones, 2016

Así mismo, el número de municipios conectados incrementó hasta llegar a 1.075 en el 2016 y el número de terminales en las instituciones educativas públicas también aumentó. En el pasado había 24 niños por terminal, y en la actualidad solo 4. Esta tendencia en el incremento del uso de las TIC también se ve evidenciada en el número de empresas de dicho sector, el cual pasó de 2.657 a 5.404, y las Mipymes se multiplicaron del 7% al 75%.

En el mismo sentido, aproximadamente desde el año 2005, Colombia se ha comprometido en la misma medida a fortalecer la seguridad de información, es por esto que a través del Decreto 1078 de 2015 se da obligatoriedad a las Entidades del Estado para implementar el Modelo de Seguridad y Privacidad de TI del Ministerio TIC.

Si bien este aumento en la conectividad en Colombia ha traído consigo innumerables beneficios para el país, también se han incrementado las amenazas cibernéticas, las vulnerabilidades y los incidentes digitales, afectando la seguridad de los ciudadanos, las organizaciones públicas y privadas, e incluso infraestructuras que hacen parte de los intereses de la nación. Las técnicas y objetivos de los ataques cibernéticos se han sofisticado, teniendo como consecuencia una mayor dificultad para su oportuna detección.

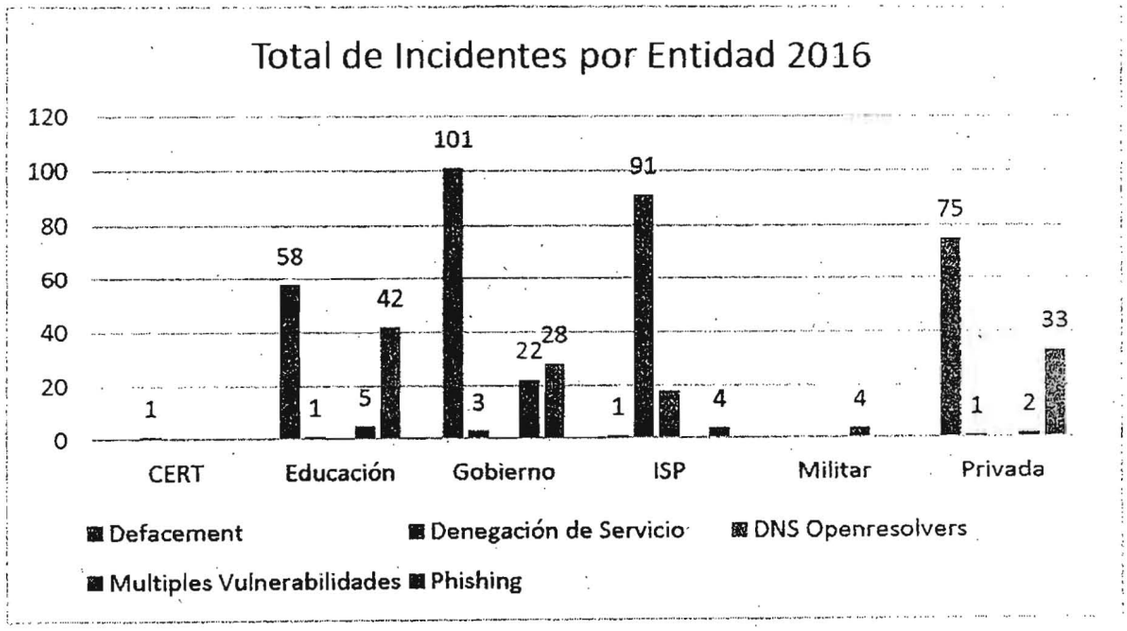
Durante los últimos años, Colombia ha sido foco de interés para distintos ataques cibernéticos, los cuales se han sofisticado trayendo consigo el incremento de la efectividad de los mismos y una mayor

dificultad para su oportuna detección. Escenario que preocupa al Gobierno nacional toda vez que las condiciones para desarrollar actividades socioeconómicas en el país cada día se soportan más en el uso de las TIC, y los incidentes digitales en Colombia afectan a varios agentes y sectores (Gráfico 2 y 3).

Gráfico 2. Sectores afectados en Colombia por incidentes digitales 2016.

	Tipo de Entidad						
Tipo de Incidente	CERT	Educación	Gobierno	ISP	Militar	Privada	Total
Defacement		58	101	1		75	235
Denegación de Servicio	1	1	3	91		1	97
DNS Openresolvers				18			18
Multiples Vulnerabilidades		5	22		4	2	33
Phishing		42	28	4		33	107
Total	**1**	**106**	**154**	**114**	**4**	**111**	**490**

Gráfico 3. Total, incidentes digitales por Entidad 2016.



Fuente: colCERT, 2016.

C. Marco Normativo Nacional

El país viene desarrollando Instrumentos Normativos que contemplan temáticas relacionadas con la seguridad de la información, la ciberseguridad y la ciberdefensa las cuales se relacionan en ésta marco normativo.

En el año 2009 se expidió la Ley 1273 "*Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "de la protección de la información y de los datos" – y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones*". Se crearon los siguientes tipos penales: Capítulo I – "*De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos*". Este capítulo tipifica las siguientes conductas penales: Acceso Abusivo a un sistema informático, obstaculización ilegítima de sistema informático o de red de telecomunicación, interceptación de datos informáticos, daño informático, uso de software malicioso, violación de datos personales, suplantación de sitios web para capturar datos personales. Capítulo II – "*De los atentados informáticos y otras*

infracciones", este capítulo tipifica el: hurto por medios informáticos y semejantes, así como la transferencia no consentida de activos.

Por medio de la Ley 1273 se adoptan los lineamientos del Convenio de Budapest celebrado en el año 2001. La decisión, de proferir las leyes internas en concordancia al Convenio sobre Ciberdelincuencia, fue tomada por considerarse de vital importancia que los desarrollos normativos incluyeran esas directrices de la legislación europea que se habían empezado a introducir en los ordenamientos jurídicos de diferentes países; aun cuando Colombia no es parte del Consejo de Europa y aún no había sido invitada a adherirse al mismo.

Colombia cuenta con una legislación procesal penal integral y efectiva para abordar los delitos cibernéticos, reconoce los tratados internacionales con INTERPOL y EUROPOL y, específicamente, la Ley 1581 de 2012 establece un marco básico para la protección de datos, divulgación y denuncia de las violaciones de seguridad. Por su parte, dentro de las leyes de carácter ordinario se encuentran unas que regulan diversos temas asociados con la seguridad digital, el comercio electrónico, la pornografía y la explotación sexual de menores en el ciberespacio, la racionalización de trámites y procedimientos, los derechos de autor y conexos, entre otros.

D. Política Pública

En el año 2011, el Gobierno Nacional aprobó el CONPES 3701 en el cual establecieron los lineamientos de política de ciberseguridad y ciberdefensa. Este documento establece las medidas que deben adoptar las entidades que tengan acceso al manejo de la información para contrarrestar el incremento de las amenazas informáticas, dentro de las cuales se establecieron normas técnicas y estándares nacionales e internacionales, así como iniciativas internacionales sobre protección de infraestructura crítica y ciberseguridad.

En abril del 2016 se aprobó el CONPES 3854 de Seguridad Digital Integral, en el que se estableció la implementación en cinco ejes : i) Establecer un marco institucional claro en torno a la seguridad digital, basado en la gestión de riesgos; ii) Crear las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital; iii) Fortalecer la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y trasnacional, con un enfoque de gestión de riesgos; iv) Fortalecer la defensa y soberanía nacional en el entorno digital con un enfoque de gestión de riesgos; y, v) Impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional. Dentro del CONPES 3854, se manifestó que la política de Ciberseguridad y Ciberdefensa adoptada por Colombia, debe ser complementada para responder adecuadamente a los nuevos tipos de incertidumbres e incidentes digitales y, adicional a lo anterior, se puso en evidencia que Colombia dispone de un marco normativo nacional disperso en torno a la seguridad digital que comprende leyes, decretos y otros actos expedidos bajo condiciones diferentes a las actuales, por lo cual se creó la política nacional de seguridad digital.

Para cumplir con los objetivos establecidos en los frentes expuestos en la Política Nacional de Seguridad Digital se establecieron diferentes estrategias. En concreto, para impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional se planteó la búsqueda de la adhesión de Colombia a diferentes convenios internacionales, dentro del cual se resaltó el Convenio de Budapest.

II. DESCRIPCION DEL ACUERDO

A. Objeto del Acuerdo

El Convenio del Consejo de Europa tiene por objeto la materialización de una política criminal común en materia de ciberdelincuencia mediante la adopción de los siguientes lineamientos:

- Intensificación de la cooperación entre Estados y su relación con el sector privado con el fin de prevenir la comisión de ilícitos en las redes informáticas.
- Adopción de la legislación interna pertinente, que permita combatir las amenazas a bienes jurídicos tutelados como la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, protegiendo en general los intereses vinculados al desarrollo de las tecnologías de la información.

B. Explicación del Articulado

El articulado del "Convenio de Budapest" está separado en las siguientes secciones:

i. Legislación sustantiva

Con el objeto de construir una Política Criminal común, encaminada a sancionar la criminalidad en el ciberespacio, el "*Convenio de Budapest*" estipula en los artículos 2 a 12 los tipos penales pertinentes para enfrentar este fenómeno. Los Estados Parte adquieren la obligación de adecuar su legislación interna a las exigencias estipuladas en dichos instrumentos, relativas a los temas de acceso ilícito, interceptación ilícita, ataques a la integridad de los datos, ataques a la integridad del sistema, abuso de los dispositivos, falsificación informática, fraude informático, delitos relacionados con la pornografía infantil, delitos relacionados con infracciones de la propiedad intelectual, y responsabilidad de las personas jurídicas. En el anexo I, se establece un cuadro comparativo con los tipos penales establecidos en el Convenio y con legislación promulgada al respecto.

En este tipo de conductas el sujeto pasivo, es decir la víctima del ilicito, puede ser cualquier persona natural o jurídica que sea dueña de un sistema de procesamiento de información.

ii. Legislación procesal

En los artículos 16 a 21 del Convenio, se estipulan procedimientos y poderes para las autoridades públicas, que también deben ser adoptados por los Estados parte en su legislación procesal interna. En el anexo II se establece un cuadro comparativo que la fecha tiene Colombia con lo establecido en el Convenio.

Las obligaciones impuestas por la normatividad en mención, se resumen en los siguientes 4 puntos:

a) Adoptar medidas para garantizar la conservación inmediata de "datos informáticos almacenados" y la divulgación de los denominados "datos de tráfico".
b) Otorgar facultades a las autoridades competentes, para que puedan solicitar a los proveedores de servicios y demás particulares la entrega de datos almacenados en su poder.
c) Disponer de medios idóneos para interceptar y compendiar en tiempo real "datos de tráfico" asociados con una comunicación particular.
d) Expedir la regulación pertinente, que habilite a sus autoridades a acceder y decomisar, cualquier sistema o soporte de almacenamiento informático.

iii. Cooperación internacional

El Convenio estipula la aplicación de instrumentos "*para luchar de forma efectiva contra dichos delitos*[1]*, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones que permitan una cooperación internacional rápida y fiable*", tomando como base los acuerdos de legislación uniforme o recíproca de los Estados, y el propio derecho interno de las partes a efectos de investigar o realizar procedimientos conjuntos relativos a los delitos relacionados con sistemas y datos informáticos o para obtener pruebas en formato electrónico de delitos.

Se busca entonces, instar a los Estados Parte a cooperar de la manera más amplia posible, por lo que Colombia se comprometería a dar trámite a las solicitudes de asistencia para la investigación y recolección de materia probatoria. Asimismo, adquiriría las obligaciones para conservar y comunicar datos informáticos almacenados de interés para los Estados partes, prestar asistencia concerniente al acceso trasfronterizo de los mismos y a establecer un punto de contacto localizable las 24 horas del día, los siete días de la semana.

III. RESERVAS

Se formulará una reserva al artículo 14 del tratado, con miras a proteger los derechos constitucionales del habeas data y la intimidad personal. En dicho postulado normativo se faculta a los Estados a reservarse el derecho de aplicar las medidas establecidas en el artículo 20 del Convenio relativo a "Obtención en tiempo real de datos relativos al tráfico", pero únicamente para ciertas categorías de delitos especificados en la reserva.

También se plantea la posibilidad de reservar la aplicación del artículo 21, concerniente a la "Interceptación de datos relativos al contenido" en los casos en que un sistema informático:

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

Estas reservas protegerían posibles vulneraciones a derechos establecidos como fundamentales en la Constitución Política de Colombia ampliamente desarrollados por la Corte Constitucional.

Al respecto del derecho a la Intimidad Personal, la Corte ha dispuesto lo siguiente:

> *"Se trata de un derecho "general, absoluto, extrapatrimonial, inalienable e imprescriptible y que se pueda hacer valer "erga omnes", vale decir, tanto frente al Estado como a los particulares. En consecuencia, toda persona, por el hecho de serlo, es titular a priori de este derecho y el único legitimado para permitir la divulgación de datos concernientes a su vida privada. Su finalidad es la de asegurar la protección de intereses morales; su titular no puede renunciar total o definitivamente a la intimidad pues dicho acto estaría viciado de nulidad absoluta. Este derecho, que se deduce de la dignidad humana y de la natural tendencia de toda persona a la libertad, a la autonomía y a la auto conservación, protege el ámbito privado del individuo y de su familia como el núcleo humano más próximo"*[2]

---

[1] "Actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, mediante la tipificación de esos actos"

[2] Ver: Sentencia C-640/10, agosto 18 de 2010, Bogotá,D.C.

Por otro lado, en relación al Habeas Data, la Corte Constitucional en sentencia T-358 de 2014 ha considerado que en *la jurisprudencia constitucional, el derecho al habeas data fue primero interpretado:*

> *"como una garantía del derecho a la intimidad, de allí que se hablara de la protección de los datos que pertenecen a la vida privada y familiar, entendida como la esfera individual impenetrable en la que cada cual puede realizar su proyecto de vida y en la que ni el Estado ni otros particulares pueden interferir.*
>
> [...]
>
> *[D]esde los primeros años de la nueva Carta, surgió al interior de la Corte una segunda línea interpretativa que consideraba el habeas data una manifestación del libre desarrollo de la personalidad. Según esta línea, el habeas data tiene su fundamento último "(...) en el ámbito de autodeterminación y libertad que el ordenamiento jurídico reconoce al sujeto como condición indispensable para el libre desarrollo de la personalidad y en homenaje justiciero a su dignidad.""*

A partir de 1995, surge una tercera línea interpretativa que es la que ha prevalecido desde entonces y que apunta al habeas data como un derecho autónomo, en que el núcleo del derecho al habeas data está compuesto por la autodeterminación informática y la libertad –incluida la libertad económica. Este derecho como fundamental autónomo, requiere para su efectiva protección de mecanismos que lo garanticen, los cuales no sólo deben pender de los jueces, sino de una institucionalidad administrativa que además del control y vigilancia tanto para los sujetos de derecho público como privado, aseguren la observancia efectiva de la protección de datos y, en razón de su carácter técnico, tenga la capacidad de fijar política pública en la materia, sin injerencias políticas para el cumplimiento de esas decisiones.

Tomando en cuenta los postulados precitados, al realizar la reserva del artículo 14, también se evitaría una posible declaratoria de inexequibilidad por parte de la Corte Constitucional, en el marco del control previo, automático e integral.

IV. IMPORTANCIA DEL CONVENIO DE BUDAPEST PARA COLOMBIA

La expansión de las amenazas en el ciberespacio, así como la utilización de nuevas tecnologías para generar amenazas informáticas, constituyen una preocupación común a todos los países, dado que impactan de manera significativa la seguridad de la información, en los ámbitos tanto público como privado.

Los fenómenos de criminalidad que afectan la Ciberseguridad son generados, en muchas ocasiones, por actores que se encuentran en una jurisdicción geográfica diferente en la que se cometen los delitos, por lo que las pruebas de un acto delictivo no son accesibles sin la colaboración judicial y técnica de las legítimas autoridades públicas que rigen sobre ese territorio. Por lo tanto, en este marco y en los casos que suponen la utilización de redes de comunicación, la cooperación internacional es esencial para prevenir y enfrentar cualquier acto delictivo en materia cibernética, por ello Colombia debe adherirse al Convenio sobre la ciberdelincuencia del Consejo de Europa.

Este es el único Instrumento internacional que cubre todas las áreas relevantes de la legislación sobre ciberdelincuencia –derecho penal, derecho procesal y cooperación internacional– y trata con carácter prioritario una política penal contra la ciberdelincuencia en cada uno de los países miembros. El Convenio de Budapest, permite no sólo avanzar en temas de cooperación internacional contra delitos

informáticos, sino también fortalecer las leyes y regulaciones nacionales contra el ciberdelito de todo nivel.

Por las anteriores consideraciones, el Gobierno Nacional, a través de la Ministra de Relaciones Exteriores, el Ministro de Justicia y del Derecho, el Ministro de Defensa Nacional y el Ministro de Tecnologías de la Información y las Comunicaciones, solicitan al Honorable Congreso de la República aprobar el Proyecto de Ley "Por medio de la cual se aprueba el *«Convenio sobre la Ciberdelincuencia»*, adoptado el 23 de noviembre de 2001, en Budapest."

De los Honorables Congresistas,

MARÍA ANGELA HOLGUÍN CUÉLLAR
Ministra de Relaciones Exteriores

LUIS CARLOS VILLEGAS ECHEVERRI
Ministro de Defensa Nacional

ENRIQUE GIL BOTERO
Ministro de Justicia y del Derecho

DAVID LUNA
Ministro de Tecnologías de la Información y las Comunicaciones

SENADO DE LA REPÚBLICA
Secretaría General (Art. 139 y ss Ley 5ª de 1.992)

El día 01 del mes Agosto del año 2017 se radicó en este despacho el proyecto de ley N°. 59 Acto Legislativo N°. _____ con todos y cada uno de los requisitos constitucionales y legales por: Dra María Angela Holguín Cuellar, Dr. Luis Carlos Villegas Echeverri, Dr. Enrique Gil Botero, Dr. David Luna

SECRETARIO GENERAL

RAMA EJECUTIVA DEL PODER PÚBLICO
PRESIDENCIA DE LA REPÚBLICA
BOGOTÁ D.C., 08 JUN 2017
AUTORIZADO. SOMÉTASE A LA CONSIDERACIÓN DEL HONORABLE CONGRESO DE LA REPÚBLICA PARA LOS EFECTOS CONSTITUCIONALES
(Fdo.) JUAN MANUEL SANTOS CALDERON
MINISTRA DE RELACIONES EXTERIORES
(Fdo.) MARÍA ÁNGELA HOLGUÍN CUÉLLAR

DECRETA:

ARTÍCULO PRIMERO: Apruébase el *«Convenio sobre la Ciberdelincuencia»*, adoptado el 23 de noviembre de 2001, en Budapest.

ARTÍCULO SEGUNDO: De conformidad con lo dispuesto en el artículo 1° de la Ley 7ª de 1944, el *«Convenio sobre la Ciberdelincuencia»*, adoptado el 23 de noviembre de 2001, en Budapest, que por el artículo primero de esta Ley se aprueba, obligará a la República de Colombia a partir de la fecha en que se perfeccione el vínculo internacional respecto del mismo.

ARTÍCULO TERCERO: La presente Ley rige a partir de la fecha de su publicación.

Dada en Bogotá D.C., a los

Presentado al Honorable Congreso de la República por la Ministra de Relaciones Exteriores, el Ministro de Justicia y del Derecho, el Ministro de Defensa Nacional y el Ministro de Tecnologías de la Información y las Comunicaciones.

MARÍA ÁNGELA HOLGUÍN CUÉLLAR
Ministra de Relaciones Exteriores

LUIS CARLOS VILLEGAS ECHEVERRI
Ministro de Defensa Nacional

ENRIQUE GIL BOTERO
Ministro de Justicia y del Derecho

DAVID LUNA
Ministro de Tecnologías de la Información y las Comunicaciones

SENADO DE LA REPÚBLICA

Secretaría General (Art. 139 y ss Ley 5ª de 1.992)

El día 01 del mes Agosto del año 2017

se radicó en este despacho el proyecto de Ley

N°. 59 Acto Legislativo N°. _____, con todos y

cada uno de los requisitos constitucionales y legales

por: Dra. Maria Angela Holguin Cuellar, D. Luis Carlos

Echeverri, D. Enrique Gil Botero, D. David Luna

SECRETARIO GENERAL

* * *

LEY 424 DE 1998

(enero 13)

por la cual se ordena el seguimiento a los convenios internacionales suscritos por Colombia

El Congreso de Colombia

DECRETA:

Artículo 1º. El Gobierno Nacional a través de la Cancillería presentará anualmente a las Comisiones Segundas de Relaciones Exteriores de Senado y Cámara, y dentro de los primeros treinta días calendario posteriores al período legislativo que se inicia cada 20 de julio, un informe pormenorizado acerca de cómo se están cumpliendo y desarrollando los Convenios Internacionales vigentes suscritos por Colombia con otros Estados.

Artículo 2º. Cada dependencia del Gobierno nacional encargada de ejecutar los Tratados Internacionales de su competencia y requerir la reciprocidad en los mismos, trasladará la información pertinente al Ministerio de Relaciones Exteriores y este, a las Comisiones Segundas.

Artículo 3º. El texto completo de la presente ley se incorporará como anexo a todos y cada uno de los Convenios Internacionales que el Ministerio de Relaciones Exteriores presente a consideración del Congreso.

Artículo 4º. La presente ley rige a partir de su promulgac

El Presidente del honorable Senado de la República.

Amylkar Acos

El Secretario General del honorable Senado de la Repúbl

Pedro Puma

El Presidente de la honorable Cámara de Representantes,

Carlos Ardila B

El Secretario General de la honorable Cámara de Represe

Diego Vi

REPUBLICA DE COLOMBIA-GOBIERNO NACIO

Publíquese y ejecútese.

Dada en Santa Fe de Bogotá, D. C., a 13 de enero de 199

ERNESTO SAMPER

La Ministra de Relaciones Exteriores,

María Emma Me

* * *

RAMA EJECUTIVA DEL PODER PÚBLICO
PRESIDENCIA DE LA REPUBLICA
BOGOTÁ, D.C., 08 JUN. 2017
AUTORIZADO. SOMÉTASE A LA CONSIDERACION DEL HONORABLE CONGRESO DE LA REPÚBLICA PARA LOS EFECTOS CONSTITUCIONALES
(Fdo.) JUAN MANUEL SANTOS CALDERON
MINISTRA DE RELACIONES EXTERIORES
(Fdo.) MARÍA ANGELA HOLGUÍN CUÉLLAR

DECRETA:

ARTÍCULO PRIMERO: Apruébase el *«Convenio sobre la Ciberdelincuencia»,* adoptado el 23 de noviembre de 2001, en Budapest.

ARTÍCULO SEGUNDO: De conformidad con lo dispuesto en el artículo 1° de la Ley 7ª de 1944, el *«Convenio sobre la Ciberdelincuencia»,* adoptado el 23 de noviembre de 2001, en Budapest, que por el artículo primero de esta Ley se aprueba, obligará a la República de Colombia a partir de la fecha en que se perfeccione el vínculo internacional respecto del mismo.

ARTÍCULO TERCERO: La presente ley rige a partir de la fecha de su publicación.

EL PRESIDENTE DEL H. SENADO DE LA REPUBLICA

EFRAIN JOSE CEPEDA SARABIA

EL SECRETARIO GENERAL DEL H. SENADO DE LA REPUBLICA

GREGORIO ELJACH PACHECO

LA PRESIDENTA (E) DE LA H. CÁMARA DE REPRESENTANTES

LINA MARIA BARRERA RUEDA

EL SECRETARIO GENERAL DE LA H. CÁMARA DE REPRESENTANTES

JORGE HUMBERTO MANTILLA SERRANO

LEY No. 1928

POR MEDIO DE LA CUAL SE APRUEBA EL "*CONVENIO SOBRE LA CIBERDELINCUENCIA*", ADOPTADO EL 23 DE NOVIEMBRE DE 2001, EN BUDAPEST.

REPÚBLICA DE COLOMBIA – GOBIERNO NACIONAL
COMUNÍQUESE Y CÚMPLASE

EJECÚTESE, previa revisión de la Corte Constitucional, conforme al artículo 241-10 de la Constitución Política.

Dada en Bogotá, D.C., a los **24 JUL 2018**

La Ministra de Educación Nacional de la República de Colombia, delegataria de funciones Presidenciales, mediante Decreto No. 1255 de 2018

LA VICEMINISTRA DE RELACIONES EXTERIORES DEL MINISTERIO DE RELACIONES EXTERIORES, ENCARGADA DE LAS FUNCIONES DEL DESPACHO DE LA MINISTRA DE RELACIONES EXTERIORES,

PATTI LONDOÑO JARAMILLO

EL MINISTRO DE JUSTICIA Y DEL DERECHO,

ENRIQUE GIL BOTERO

EL MINISTRO DE DEFENSA NACIONAL,

LUIS CARLOS VILLEGAS ECHEVERRI

EL VICEMINISTRO DE CONECTIVIDAD Y DIGITALIZACIÓN DEL MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES, ENCARGADO DEL EMPLEO DEL DESPACHO DEL MINISTRO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES,

JUAN SEBASTIAN ROZO RENGIFO