Sentencia C-224/19

CONVENIO SOBRE LA CIBERDELINCUENCIA-Se ajusta a la constitución política

CONTROL DE CONSTITUCIONALIDAD EN MATERIA DE TRATADOS Y LEYES APROBATORIAS DE TRATADOS-Competencia de la Corte Constitucional/CONTROL DE CONSTITUCIONALIDAD DE LEY APROBATORIA DE TRATADO-Características

Según lo ha establecido reiterada jurisprudencia de esta Corporación, el control que ejerce la Corte Constitucional sobre los tratados públicos y sus leyes aprobatorias, se caracteriza por ser: "(i) previo al perfeccionamiento del tratado, pero posterior a la aprobación del Congreso y a la sanción gubernamental; (ii) automático, pues debe ser enviada directamente por el Presidente de la República a la Corte Constitucional dentro de los seis días siguientes a la sanción gubernamental; (iii) integral, en la medida en que la Corte debe analizar tanto los aspectos formales como los materiales de la ley y el tratado, confrontándolos con todo el texto constitucional; (iv) tiene fuerza de cosa juzgada; (v) es una condición sine qua non para la ratificación del correspondiente acuerdo; y (vi) cumple una función preventiva, pues su finalidad es garantizar tanto la supremacía de la Constitución como el cumplimiento de los compromisos internacionales del Estado colombiano."

LEYES APROBATORIAS DE TRATADOS INTERNACIONALES-Procedimiento de formación previsto para leyes ordinarias/LEYES APROBATORIAS DE TRATADOS INTERNACIONALES-Trámite legislativo

CONTROL DE CONSTITUCIONALIDAD DE TRATADO INTERNACIONAL Y LEY APROBATORIA-Suscripción del tratado y aprobación presidencial

CONSULTA PREVIA DE COMUNIDADES Y GRUPOS ETNICOS-Procedimiento previo antes de un trámite legislativo en el que se adopten medidas que puedan afectarlas directamente

DERECHO FUNDAMENTAL A LA CONSULTA PREVIA DE LEYES APROBATORIAS DE TRATADOS INTERNACIONALES-Jurisprudencia constitucional

CONTROL DE CONSTITUCIONALIDAD EN MATERIA DE TRATADOS Y LEYES APROBATORIAS DE TRATADOS-Control formal y material

CONVENIO SOBRE LA CIBERDELINCUENCIA-Trámite legislativo

TRATADO INTERNACIONAL Y LEY APROBATORIA-Cumplimiento de requisitos constitucionales y legales en su trámite legislativo

CONVENIO SOBRE LA CIBERDELINCUENCIA-Control material

CONVENIO SOBRE LA CIBERDELINCUENCIA-Contenido

DERECHO A LA INTIMIDAD PERSONAL Y FAMILIAR-Jurisprudencia constitucional

DERECHO A LA INTIMIDAD-Alcance y contenido

DERECHO A LA INTIMIDAD-Principios que lo protegen/PRINCIPIO DE LIBERTAD-Concepto/PRINCIPIO DE FINALIDAD-Concepto/PRINCIPIO DE NECESIDAD-Concepto/PRINCIPIO DE VERACIDAD-Concepto/PRINCIPIO DE INTEGRIDAD-Concepto

INTERCEPTACION DE COMUNICACIONES-Desarrollo normativo

INTERCEPTACION DE COMUNICACIONES-Desarrollo jurisprudencial

DERECHO AL HABEAS DATA-Concepto

DERECHO AL HABEAS DATA EN TRATAMIENTO DE DATOS PERSONALES-Principios y garantías constitucionales

Referencia: Expediente LAT-455

Revisión oficiosa de la Ley 1928 de 2018 "Por medio de la cual se aprueba el convenio sobre la ciberdelincuencia, adoptado el 23 de noviembre de 2001, en Budapest".

Magistrada Ponente:

CRISTINA PARDO SCHLESINGER

Bogotá, D. C., veintidós (22) de mayo de dos mil diecinueve (2019)

La Sala Plena de la Corte Constitucional, integrada por los magistrados Gloria Stella Ortiz

Delgado, quien la preside, Carlos Bernal Pulido, Diana Fajardo Rivera, Luis Guillermo Guerrero Pérez, Alejandro Linares Cantillo, Antonio José Lizarazo Ocampo, Cristina Pardo Schlesinger, José Fernando Reyes Cuartas y Alberto Rojas Ríos, en cumplimiento de sus atribuciones constitucionales y de los requisitos y trámite establecidos en el Decreto 2067 de 1991, ha proferido la siguiente

SENTENCIA

Dentro del proceso de revisión de constitucionalidad de la Ley 1928 de 2018, "Por medio de la cual se aprueba el convenio sobre la ciberdelincuencia, adoptado el 23 de noviembre de 2001, en Budapest".

I. ANTECEDENTES

De acuerdo con lo previsto en el numeral 10 del artículo 241 de la Constitución Política, el treinta (30) de julio de dos mil dieciocho (2018) la Secretaría Jurídica de la Presidencia de la República remitió a la Secretaría General de esta Corporación, mediante oficio número OFI18-00084528/JMSC110200, una fotocopia autenticada de la Ley 1928 de 2018, para su revisión constitucional.

En Auto del diecisiete (17) de agosto de dos mil dieciocho (2018), la Magistrada Sustanciadora avocó conocimiento de la ley de la referencia, y con el objeto de realizar el estudio de constitucionalidad de la disposición legal referida, decretó la práctica de pruebas tendientes a conocer el trámite legislativo de aprobación de la Ley 1928 de 2018, para lo cual se ofició a los Secretarios Generales del Senado de la República y de la Cámara de Representantes, a los Secretarios Generales de la Comisión Segunda del Senado de la República y de la Cámara de Representantes, así como al Ministerio de Relaciones Exteriores solicitándoles los respectivos documentos.

Finalmente, en la citada providencia se ordenó comunicar la iniciación del proceso e invitar al Ministerio de Relaciones Exteriores, al Ministerio de Tecnologías de la Información y las Comunicaciones, al Ministerio de Justicia y del Derecho, al Ministerio de Defensa Nacional, al Ministerio del Interior, a la Fiscalía General de la Nación, a la Cámara Colombiana de Comercio Electrónico, a la Delegatura para la Protección de Datos Personales de la Superintendencia de Industria y Comercio, a la Superintendencia Financiera de Colombia, al

Centro Cibernético Judicial de la Policía Nacional, a la Delegada en Asuntos Constitucionales y Legales de la Defensoría del Pueblo, a la Delegada para la Infancia, la Juventud y Adulto Mayor de la Defensoría del Pueblo, al Instituto Colombiano de Bienestar Familiar, a la Asociación Bancaria y de Entidades Financieras de Colombia, a la Asociación Colombiana de la Propiedad Intelectual, a la Comisión Colombiana de Juristas, a Public Policy and Government Google Colombia, a las Facultades de Derecho de la Universidad del Rosario, de la Universidad Sergio Arboleda, de la Universidad Nacional de Colombia, a la Facultad de Finanzas, Gobierno y Relaciones Internacionales de la Universidad Externado de Colombia, al Departamento de Derecho y Dirección de Investigaciones de la Universidad ICESI y a la Universidad de los Andes para que, si lo estimaban conveniente, participaran en el debate jurídico a efectuarse.

Posteriormente, al advertir la falta de algunas pruebas sobre el trámite legislativo, mediante providencia del catorce (14) de septiembre de dos mil dieciocho (2018), el despacho sustanciador requirió al Secretario General del Senado de la República para que diera cumplimiento a lo ordenado en el numeral segundo del Auto del diecisiete (17) de agosto de la misma anualidad, relativo a la remisión a esta Corporación y con destino al proceso de la referencia de los documentos contentivos del trámite legislativo de aprobación de la Ley 1928 de 2018 en esa Corporación.

Cumplidos los trámites constitucionales y legales propios de esta clase de juicios, y previo concepto del Procuraduría General de la Nación, procede la Corte a realizar el estudio de constitucionalidad del instrumento internacional y de su ley aprobatoria.

II. TEXTO DE LA NORMA BAJO EXAMEN

A continuación se transcribe el texto completo de la ley aprobatoria del Convenio que se revisa[1]:

“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;

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:

1) toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar por medio de un sistema informático, y

2) 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:

1.

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

iii. 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:

1.

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.

1.

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 15.

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.

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:

b.

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.

2.

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

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 aplicar· 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 informar· a su debido tiempo del resultado final a la Parte requirente. Dichas autoridades tomaron su decisión y efectuaron 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.

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.

5.

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, informar· 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, quedar· 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 comunicar 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 crear· 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.

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 estudiar·, 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. Deber· motivarse cualquier denegación o aplazamiento de la asistencia solicitada. La Parte requerida informar 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 enviar· 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 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 informar 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.

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 determinar· 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.

4.

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, informar· de ello sin demora a la Parte requirente, la cual decidir· 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 prestaran 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 regir· 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.

Las Partes se prestaran 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 velar· por garantizar la coordinación con dicha autoridad o autoridades con carácter urgente.

3. Cada Parte garantizar· 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 depositaran 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 aplicar· 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, deber· 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.

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.

2.

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 desempeorar 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".

III. INTERVENCIONES

El Ministerio de Relaciones Exteriores, a través de la Directora de Asuntos Jurídicos Internacionales, intervino en el proceso de la referencia y solicitó declarar exequible la Ley 1928 de 2018.

Inicialmente, realizó una breve reseña sobre el objeto, el estado actual, la importancia y la pertinencia del Convenio sobre la Ciberdelincuencia, destacando que el mismo es una guía para que cualquier país desarrolle una legislación nacional integral contra el delito cibernético en un marco de cooperación internacional entre los Estados Parte. Señaló que, en la actualidad, el citado instrumento ha sido firmado por 46 de los 47 Estados miembros del Consejo de Europa. De ese grupo, 42 países lo han ratificado.

La Directora de Asuntos Jurídicos Internacionales del Ministerio de Relaciones Exteriores indicó que la comunidad internacional se ve enfrentada a nuevas y cada vez más amenazas en el ciberespacio, así como a avanzadas tecnologías para su generación en medio de un aumento de herramientas informáticas para ello. En esa medida, afirmó que es una problemática que comporta un carácter transnacional, por lo que constituye una preocupación común de todos los Estados, pues impacta de manera significativa la seguridad de la información, en los ámbitos tanto público como privado.

Sostuvo que los fenómenos de criminalidad que afectan a la ciberseguridad, en muchas ocasiones, son generados por actores que se encuentran en una jurisdicción geográfica diferente a 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, adujo que en los casos en que sea necesaria la

utilización de redes de comunicación, la cooperación internacional es esencial para prevenir y enfrentar cualquier conducta ilegal en materia cibernética.

Afirmó que "Colombia debe adherirse al Convenio sobre la Ciberdelincuencia del Consejo de Europa", pues "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 Estados miembro. 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"[2].

Para la cartera interviniente, el Convenio objeto de análisis resulta pertinente ya que busca dar cumplimiento a los fines esenciales del Estado colombiano, consagrados en el artículo 2 de la Constitución Política en cuanto a la protección de derechos y libertades de la población y persigue la garantía de los derechos fundamentales constitucionales del artículo 15 superior, relacionados con el derecho a la intimidad personal, familiar y al buen nombre.

Adicionalmente, el Ministerio de Relaciones Exteriores realizó una sucinta reseña del Convenio sobre la Ciberdelincuencia; específicamente, se pronunció sobre la terminología, las medidas que deberán adoptarse a nivel nacional, la cooperación internacional, las disposiciones finales y las reservas que el numeral 3 del artículo 14 del citado convenio le otorga al Estado colombiano con miras a proteger los derechos constitucionales del habeas data y la intimidad personal, en consonancia con la línea jurisprudencial que la Corte Constitucional ha desarrollado.

Finalmente, se refirió al trámite de aprobación interna de la Ley 1928 de 2018 por parte de Colombia, señaló que el entonces Presidente de la República, Juan Manuel Santos Calderón, impartió la respectiva Aprobación Ejecutiva el 8 de junio de 2017, con sujeción a lo previsto en el artículo 189, numeral 2 de la Constitución Política.

En virtud de la aludida autorización, el Gobierno Nacional, por intermedio de los entonces Ministros de Relaciones Exteriores, Defensa Nacional, Justicia y del Derecho y Tecnologías de la Información y Comunicaciones, y en consonancia con los artículos 150, numeral 2 y

224 de la Constitución, presentó el 1 de agosto de 2017, ante la Secretaría General del Senado de la República, el Proyecto de ley.

Surtidos los respectivos debates, el Congreso aprobó la Ley 1928 del 24 de julio de 2018. Posteriormente, la misma fue sancionada por el Presidente de la República y publicada en el Diario Oficial No. 50.664[3].

Por lo anteriormente expuesto, la Directora de Asuntos Jurídicos Internacionales del Ministerio de Relaciones Exteriores solicitó la declaratoria de constitucionalidad de la Ley 1928 de 2018, al considerar que el "Convenio sobre la Ciberdelincuencia", cumplió con los requisitos formales previstos en la Constitución Política para su suscripción y aprobación legislativa y se ajusta a los principios y postulados que gobiernan al Estado colombiano y a su política exterior.

2. Ministerio de Defensa

El Ministerio de Defensa solicitó a la Corte Constitucional declarar la constitucionalidad de la Ley 1928 de 2018, con fundamento en los siguientes argumentos:

Indicó que la norma referida, aprobatoria del Convenio sobre la Ciberdelincuencia, cumplió con las exigencias constitucionales formales. De igual manera, resaltó que el contenido material consulta los principios y postulados que gobiernan al Estado Social de Derecho y su política exterior.

Señaló que la aprobación del convenio analizado como parte de la legislación interna resulta de significativa importancia para fortalecer las capacidades técnicas y operativas que actualmente la Policía Nacional viene desplegando, en materia de seguridad digital y ciberseguridad.

Refirió que la incorporación al ordenamiento jurídico interno del Convenio que nos ocupa traería ventajas en lo que corresponde a: liderazgo sectorial en Latinoamérica sobre temas CIBER, cooperación internacional, fortalecimiento de herramientas jurídicas, reconocimiento internacional, mejoramiento en los procedimientos investigativos alineados al marco internacional, respuesta de solicitudes internacionales, capacitaciones e intercambio de conocimiento, herramientas tecnológicas y alianzas estratégicas.

La apoderada especial del Ministerio de Defensa afirmó que el Convenio sobre la Ciberdelincuencia permitirá contar con el marco normativo necesario para realizar las gestiones propias que conlleva la relación de cooperación con las organizaciones internacionales. Asimismo, sostuvo que esta relación está enfocada en fortalecer las capacidades de las Fuerzas Militares de Colombia, mediante el establecimiento de estándares que permiten la interoperabilidad, en diversos frentes, entre las Fuerzas Armadas colombianas y las de los países que hacen parte de esta alianza.

Adujo que con la adopción de estos elevados estándares, que abarcan aspectos logísticos, técnicos y operativos, se está dando cumplimiento al diseño de definir una hoja de ruta que determine el futuro de las Fuerzas Militares y de la Policía Nacional. Lo anterior, dentro de un modelo de planeación de mediano y largo plazo, que busca "definir una estructura de Fuerzas que evolucione de manera concordante con los retos operacionales futuros y que garanticen la coherencia entre el marco presupuestal existente, los principios de política, las misiones y las capacidades de la Fuerza Pública"[4].

Finalmente, la cartera interviniente resaltó que Colombia se encuentra en el marco de actuación del Convenio, pues cumple con los parámetros mínimos requeridos, y con su entrada en vigor se potencializará la ley penal, la ley de procedimiento penal y la articulación internacional en materia de lucha contra el cibercrimen, con fundamento en la no territorialidad que tiene el fenómeno, en consideración a la premisa que el ciberespacio no tiene jurisdicción.

3. Ministerio de Justicia y del Derecho

El Ministerio de Justicia y del Derecho, a través del Director de Desarrollo del Derecho y del Ordenamiento Jurídico, participó en el debate planteado y solicitó declarar la exequibilidad del Convenio de ciberdelincuencia, adoptado el 3 de noviembre de 2001 en Budapest y de la Ley 1928 de 2018 que lo aprueba.

Destacó que el propósito del Convenio firmado Budapest es global, pues tiene como objetivo la lucha de la ciberdelincuencia en todos los países del mundo. En esa medida, adujo que ese fenómeno criminal solo podrá ser eficazmente enfrentado si existe un compromiso de cooperación del mayor número de países.

Indicó que la ratificación del Tratado se justifica en la necesidad de complementar los esfuerzos de colaboración internacional y la lucha efectiva contra los actos dirigidos a la confidencialidad, a la integridad y a la disponibilidad de sistemas, así como a las redes de delitos informáticos.

Para el Ministerio de Justicia y del Derecho, desde un punto de vista material, el Convenio sobre la Ciberdelincuencia defiende fines constitucionalmente válidos y su ratificación busca materializar los lineamientos de política pública relacionados con la ciberseguridad, la ciberdefensa y la prevención de la cibercriminalidad adoptadas a través de los documentos CONPES 301 de 2011 y 3854 de 2016, en los que se precisa la necesidad de contar con estrategias complementarias, procedimentales y de cooperación internacional, entre otras, dirigidas a articular esfuerzos y consolidar una política de protección común en temas de escala y afectación global.

Finalmente, el Director de Desarrollo del Derecho y del Ordenamiento Jurídico del referido ministerio aclaró que "a pesar de no evidenciarse una eventual afectación de los bienes jurídicos tutelados por nuestra constitución se destaca el hecho de que, tal como se señala en la exposición de motivos, se formuló una reserva a los artículos 14 y 21 de la convención, a fin de complementar la protección de los derechos constitucionales de habeas data y a la intimidad"[5].

4. Superintendencia de Industria y Comercio

El Superintendente de Industria y Comercio solicitó la declaratoria de exequibilidad de la Ley 1928 de 2018, por medio de la cual se aprueba el Convenio de Budapest sobre la Ciberdelincuencia, con fundamento en los siguientes argumentos.

Aclaró que esa entidad tiene como función principal ser una autoridad de protección de datos personales; en esa medida, ejerce "la vigilancia para garantizar que en el Tratamiento (sic) de datos personales se respeten los principios, derechos, garantían y procedimientos previstos" en la Ley 1581 de 2012"[6].

Teniendo en cuenta lo anterior, afirmó que su intervención se realizaría desde una perspectiva de los aspectos involucrados en el Convenio sobre la Ciberdelincuencia respecto de datos personales.

Afirmó que la realidad socio tecnológica del siglo XXI, impulsada por la internet, requiere que los Estados cuenten con herramientas efectivas frente a un mundo cada vez más global y transfronterizo. Señaló que "internet cambio el mundo, y es necesario que el mundo cambie frente a internet porque nuestros sistemas jurídicos fueron principalmente pensados para un mundo intrafronterizo"[7].

Para la Superintendencia de Industria y Comercio el Convenio de Budapest se enfoca en el camino correcto de dotar a los Estados de instrumentos jurídicos para poder actuar frente a situaciones extraterritoriales o transfronterizas que cada vez son más cotidianas.

Indicó que el Convenio objeto de análisis incluye la necesidad de que los Estados Parte adopten medidas a nivel nacional para tipificar algunas conductas contrarias a la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos; incluso, aquellas consideradas como delitos contra la propiedad intelectual y sus derechos afines.

Adicionalmente, explicó que el Convenio de Budapest incluye instrucciones relacionadas con la cooperación internacional en materia de extradición, asistencia para la obtención de pruebas, intercambio de información y el acceso transfronterizo de datos. Por lo anterior, adujo que era necesario "hacer modificaciones sustanciales a la normatividad interna, con el fin de considerar ciertas conductas como delitos y poder, en consecuencia, realizar las investigaciones y los juicios de dichas conductas de manera eficiente y eficaz para garantizar la seguridad de los ciudadanos"[8].

Finalmente, como autoridad de protección de datos personales, recomendó tener en cuenta que la cooperación internacional de que trata el Convenio objeto de estudio debe darse siempre bajo los límites del respeto a los derechos al buen nombre, intimidad, libertad de expresión y, especialmente, el derecho a la protección de los datos de las personas.

5. Universidad Sergio Arboleda

La Universidad Sergio Arboleda, a través de docentes investigadores del Departamento de Derecho Penal, se pronunció sobre la revisión oficiosa de la Ley 1928 de 2018, aprobatoria del Convenio sobre la Ciberdelincuencia, adoptado el 23 de noviembre de 2001, y le solicitó a la Corte Constitucional declarar exequible la norma objeto de control, de conformidad con

las siguientes apreciaciones:

Sostuvo la institución de educación superior interviniente que el preámbulo del Convenio se corresponde con los lineamientos del artículo 2 de la Constitución Política, pues contribuye a lograr los fines esenciales del Estado y robustece una de las misiones de las autoridades de la Republica: "proteger a todas las personas residentes en Colombia, en su vida, honra, bienes, creencias y demás derechos y libertades"[9].

Sobre el capítulo I del Convenio sobre la Ciberdelincuencia indicó que contiene un carácter meramente descriptivo, refriéndose a los datos informáticos como una especie de información que encuentra soporte constitucional en los artículos 15 y 20 superiores y que permite su intercambio a través de "sistemas informáticos".

En relación con el capítulo II del instrumento internacional aprobado por la Ley 1928 de 2018, "medidas que deberán adoptarse a nivel nacional", manifestó que respeta la Constitución Política de 1991.

Aseguró que las funciones informáticas protegidas por los delitos que atenten contra la integridad, confiabilidad, disponibilidad, autenticidad y confidencialidad informática se inspiran en derechos fundamentales consagrados en nuestro ordenamiento constitucional como las garantías a la intimidad, al habeas data, al libre desarrollo de la personalidad o a la honra, entre otros. Adicionalmente, se indica en el escrito de intervención que "los crímenes relacionados con la pornografía infantil (art. 9 del Convenio) se dirigen a erradicar el abuso y la explotación sexual de los niños, conforme al artículo 44 superior"[10].

No obstante, la Universidad Sergio Arboleda, para preservar el postulado de necesidad de intervención, según el cual el derecho penal tiene carácter de última ratio y solo actúa ante ataques graves contra los bienes jurídicos, sugiere a esta Corporación manifestarse a favor de la reserva del apartado 2 del artículo 4 del Convenio que limita el alcance del delito de daño informático[11].

Asimismo, arguye que debe avalarse la reserva del apartado 4 del artículo 9 del Convenio analizado, pues el concepto de "pornografía infantil" debe limitarse a "las representaciones visuales de menores comportándose de una forma sexualmente explícita (es decir, a las fotos o grabaciones) y no debe ampliarse a otras representaciones en donde personas que

parecen menores comportándose de la misma manera (dibujos, grabados, esculturas, etc.)”[12].

Lo anterior, al argumentar que se podría violentar los principios de lesividad y de acto y de “caer en un Derecho Penal autor”, incompatible con el modelo de Estado colombiano.

Finalmente, se refirió al capítulo III del Convenio – Cooperación internacional. Para la universidad interviniente, este aparte del tratado encuentra respaldo en los artículos 226 y 227 de la Constitución de 1991, pues define los principios reguladores de las relaciones con los Estados Parte y promueve la integración económica, social y política con las demás naciones. Asimismo, consideró que el artículo 24 del Convenio se ajusta al artículo 35 superior en temas de extradición.

Empero, resaltó que la Corte Constitucional puede exigir la ampliación de la cláusula de reserva del apartado 4 del artículo 29 que preceptúa: “cuando una Parte Exija (sic) 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 los delitos de los previstos con a arreglo (sic) a los artículos 2 a 11 del presente Convenio(…)”[14].

IV. CONCEPTO DE LA PROCURADURÍA

GENERAL DE LA NACIÓN

En ejercicio de las competencias previstas en los artículos 242, numeral 2°, y 278, numeral 5°, del texto constitucional, así como el artículo 7 del Decreto 2067 de 1991, el señor Procurador General de la Nación, Fernando Carrillo Flórez, presentó concepto número 6486 dentro del trámite de la referencia, en el cual solicita a la Corte la declaración de exequibilidad de la norma objeto de estudio.

En cuanto al trámite del Proyecto de la ley aprobatoria, la Vista Fiscal, luego de realizar un recuento de la etapa prelegislativa y legislativa de la misma, advirtió que se ajustó a los cánones constitucionales, legales y reglamentarios. Sobre el particular, señaló que el proyecto de ley cumplió con los requisitos de presentación y publicación antes de darle trámite en la comisión respectiva, surtió los debates reglamentarios, tanto en el Senado

como en la Cámara de Representantes, y se aprobó conforme a las normas pertinentes.

En relación con el contenido material del convenio internacional, la Procuraduría General de la Nación destacó que el mismo se ajusta a las expectativas constitucionales y observa las normas superiores aplicables, en especial los artículos 15, 20, 44 y 61 de la Constitución, promoviendo la internacionalización de las relaciones mediante la celebración de tratados (arts. 9, 226 y 227 C.P.), y la efectividad de los principios, derechos y deberes consagrados en la Constitución Política.

Indicó que el propósito del Convenio bajo examen remite a "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 fenómeno de la cooperación internacional". Que en esa medida, en la Ley 1928 de 2018 se contemplan aspectos vitales para lograr la finalidad trazada sin desconocer las bases de equidad, reciprocidad y conveniencia nacional, pues fomenta la cooperación internacional y se reconoce el ámbito de los poderes y legislaciones en Colombia.

Refirió que el preámbulo del Convenio contempla "la necesidad de garantizar el debido equilibrio entre los intereses de la acción penal y el respeto de los derechos humanos fundamentales", precisión que resulta de gran relevancia, pues alude a la prevención y lucha frente a "los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos", para la protección de los datos personales y de los derechos de los menores de edad, así como a la importancia de combatir la piratería en materia de propiedad intelectual, todo lo cual guarda armonía con el ordenamiento constitucional colombiano (art. 61 C.P.).

En el mismo sentido, realizó un recuento del contenido normativo del Tratado y sostuvo que en su integralidad se encuentra ajustado a la Constitución Política. Así, consideró que las disposiciones contenidas en el Convenio sobre la Ciberdelincuencia se subordinan a las regulaciones del derecho interno y a la adopción de los tipos y sanciones acordados en los instrumentos internacionales.

Sobre la configuración de los delitos, destacó que apuntan a la salvaguardia de un bien jurídico de relevancia constitucional, pues promueven la protección de los datos y sistemas informáticos – confidencialidad, integridad y disponibilidad-, y respetan los límites

impuestos por la Constitución y desarrollados por el legislador penal.

La Procuraduría General de la Nación indicó que procede la reserva anunciada por el Estado colombiano frente a la aplicación de los artículos 20 y 21 del Convenio, conforme al artículo 14.3 ibídem, pues se ajusta al concepto 06.2018 proferido por el Consejo Superior de Política Criminal[15] al indicar que "(…) a los ojos de [ese] órgano resulta ser conveniente, pues la aplicación de estas disposiciones puede entrar en contradicción con los derechos y garantías fundamentales contempladas en la Constitución Política. Los citados artículos propenden por la obtención de datos en tiempo real, lo cual puede implicar una afectación al derecho [a] la intimidad personal, el cual en los términos de la Corte Constitucional es de carácter fundamental e inalienable, siendo el titular de este, el único legitimado para permitir la divulgación de datos relativos a su vida privada"[16].

Por último, el señor Procurador General de la Nación Concluyó que:

"La Ley 1928 del 24 de julio de 2018 cumple con los establecido en el artículo 150.16 Constitucional (aprueba el tratado internacional sin introducir modificaciones) y las reglas sobre la entrada en vigor del mismo.

En relación con el 'Convenio sobre la Ciberdelincuencia', adoptado el 23 de noviembre de 2001, en Budapest, una vez analizado su contendido (capítulo I a IV), se encuentra que se ajusta a las disposiciones de la Carta Política en las condiciones señaladas.

El Convenio desarrolla el mandato de la internacionalización de las relaciones y el respeto a la autodeterminación, sobre bases de equidad, reciprocidad y conveniencia nacional (artículos 226 y 227 de la C.P.), incluye disposiciones que despliegan los fines constitucionales (artículo 2 de la C.P.), atiende la soberanía e independencia del Estado colombiano (artículos 2, 4 y 9 de la C.P.), y guarda armonía con los preceptos superiores identificados en cada uno de los capítulos examinados"[17].

V.CONSIDERACIONES DE LA CORTE CONSTITUCIONAL

1. COMPETENCIA

De acuerdo a lo establecido en el numeral 10º del artículo 241 de la Constitución Política, la Corte Constitucional es competente para ejercer el control integral de constitucionalidad de

los tratados internacionales y de las leyes que los aprueben.

La Ley 1928 de 2018, por medio de la cual se aprueba el Convenio sobre la Ciberdelincuencia adoptado el 3 de noviembre de 2001 en Budapest, es aprobatoria de un tratado público, por lo que, tanto desde el punto de vista material como formal, esta Corporación es competente para adelantar su estudio de constitucionalidad.

Según lo ha establecido reiterada jurisprudencia de esta Corporación,[18] el control que ejerce la Corte Constitucional sobre los tratados públicos y sus leyes aprobatorias, se caracteriza por ser:

"(i) previo al perfeccionamiento del tratado, pero posterior a la aprobación del Congreso y a la sanción gubernamental; (ii) automático, pues debe ser enviada directamente por el Presidente de la República a la Corte Constitucional dentro de los seis días siguientes a la sanción gubernamental; (iii) integral, en la medida en que la Corte debe analizar tanto los aspectos formales como los materiales de la ley y el tratado, confrontándolos con todo el texto constitucional; (iv) tiene fuerza de cosa juzgada; (v) es una condición sine qua non para la ratificación del correspondiente acuerdo; y (vi) cumple una función preventiva, pues su finalidad es garantizar tanto la supremacía de la Constitución como el cumplimiento de los compromisos internacionales del Estado colombiano."

La revisión del aspecto formal del tratado internacional y de su ley aprobatoria se dirige a examinar dos aspectos: i) la validez de la representación del Estado colombiano en las fases de negociación, celebración y firma del Convenio internacional; y ii) la observancia de las reglas de trámite legislativo que precedieron a la aprobación de la ley objeto de análisis.

La Constitución Política no dispone de un procedimiento legislativo especial para la expedición de una ley aprobatoria de un tratado internacional, salvo que su trámite inicie en el Senado de la República. Por este motivo, el Congreso de la República debe seguir, en términos generales, el mismo trámite que una ley ordinaria. Desde esta perspectiva se requiere, en razón del trámite ordinario: (i) la publicación oficial del proyecto de ley; (ii) el inicio del procedimiento legislativo en la comisión constitucional correspondiente del Senado de la República[19]; (iii) la aprobación reglamentaria en los debates de las

comisiones y plenarias de cada una de las cámaras[20]; (iv) que entre el primer y segundo debate medie un lapso no inferior a ocho días y que entre la aprobación del proyecto en una de las cámaras y la iniciación del debate en la otra, transcurran por lo menos quince días[21]; (v) la comprobación del anuncio previo a la votación en cada uno de los debates; (vi) la votación nominal y pública en cada una de las células legislativas, salvo cuando se trata de votación unánime, y (vii) la sanción presidencial y la remisión del texto a la Corte Constitucional dentro de los seis días siguientes[22].

Por último, el examen de fondo consiste en confrontar las disposiciones del texto del tratado internacional objeto de análisis y su ley aprobatoria, con la totalidad del texto constitucional, a fin de determinar si se ajustan o no al ordenamiento superior.

Hechas las anteriores precisiones, pasa la Corte a examinar la constitucionalidad del tratado internacional objeto de estudio y de su ley aprobatoria, tanto en su aspecto formal como material.

2. ANÁLISIS FORMAL DE LA SUSCRIPCIÓN Y APROBACIÓN DEL ACUERDO

2.1. Suscripción del Acuerdo

Según lo ha manifestado esta Corporación[23], el control formal de constitucionalidad de los tratados internacionales y sus leyes aprobatorias incluye el examen de las facultades del representante del Estado colombiano para negociar, adoptar el articulado mediante su voto y autenticar el instrumento internacional respectivo.

La anterior verificación ha sido realizada por la Corte de acuerdo con lo previsto en los artículos 7º a 10º de la Convención de Viena sobre el Derecho de los Tratados entre Estados de 1969, incorporada al ordenamiento interno por la Ley 32 de 1985, por remisión que hace el artículo 9º de la Carta en el sentido de que las relaciones exteriores del Estado se fundamentan en el reconocimiento de los principios aceptados por Colombia.

De esta manera, el artículo 7º de la Convención de Viena sobre el Derecho de los Tratados de 1969, señala lo siguiente:

"1. Para la adopción o la autenticación del texto de un tratado, o para manifestar el consentimiento del Estado en obligarse por un tratado, se considerará que una persona

representa a un Estado:

a) Si presenta los adecuados plenos poderes, o

b) Si se deduce de la práctica seguida por los Estados interesados, o de otras circunstancias, que la intención de esos Estados han sido considerar a esa persona representante del Estado para esos efectos y prescindir de la presentación de plenos poderes.

2. En virtud de sus funciones, y sin tener que presentar plenos poderes, se considerará que representan a su Estado:

a) Los jefes de Estado, jefes de gobierno y ministros de relaciones exteriores, para la ejecución de todos los actos relativos a la celebración de un tratado;

b) Los jefes de misión diplomática, para la adopción del texto de un tratado entre el Estado acreditante y el Estado ante el cual se encuentran acreditados;

c) Los representantes acreditados por los Estados ante una conferencia internacional o ante una organización internacional o uno de sus órganos, para la adopción del texto de un tratado en tal conferencia, organización u órgano." (Subrayado fuera de texto original).

Así las cosas, el entonces Presidente de la República, Juan Manuel Santos Calderón, impartió la respectiva Aprobación Ejecutiva el 8 de junio de 2017, con sujeción a lo previsto en el artículo 189, numeral 2 de la Constitución Política, por lo que en virtud de lo establecido en

el literal a), numeral 2 del artículo 7 precitado, no fue necesaria la expedición de Plenos Poderes.

Todo lo anterior, según constancia enviada a esta Corporación, con los respectivos anexos, el 26 de octubre de 2018, por la Directora de Asuntos Jurídicos Internacionales del Ministerio de Relaciones Exteriores[24].

Adicionalmente, se adjuntó a la Corte copia autentica de la Aprobación Ejecutiva del 8 de junio 2017, por medio de la cual el entonces Presidente de la República, Juan Manuel Santos Calderón, autorizó someter a consideración del Congreso de la República el Convenio sobre la Ciberdelincuencia, adoptado el 23 de noviembre de 2001 en Budapest, Hungría[25], acto que contó con la firma de la entonces Ministra de Relaciones Exteriores, doctora María Ángela Holguín Cuellar.

De tales precisiones se concluye que la adopción del instrumento internacional satisface el requisito de forma, respecto a la calidad de la persona que debió suscribirlo, y cumpliéndose lo previsto en los artículos 189-2 y 224 de la Constitución Política.

2.2. Asunto previo: necesidad y realización de consulta previa como expresión del derecho fundamental a la participación de los grupos étnicos

La Corte Constitucional se ha pronunciado en diferentes ocasiones sobre el ejercicio del derecho a la consulta previa de leyes aprobatorias de tratados internacionales ratificados por el Estado colombiano.

Así, esta Corporación en la Sentencia C-750 de 2008[26], señaló que toda medida legislativa o administrativa que afecte de forma directa a una población étnica debe someterse a la consulta previa, como consecuencia del derecho que le asiste a dicha comunidad a decidir sobre sus prioridades en su desarrollo y preservación cultural.

Recientemente, la Corte Constitucional en la Sentencia C-048 de 2018, al efectuar la revisión oficiosa de la Ley 1844 de 2017 "por medio de la cual se aprueba el "Acuerdo de París", adoptado el 12 de diciembre de 2015, en París, Francia", reitero las reglas jurisprudenciales sobre el ejercicio del derecho a la consulta previa frente a tratados internacionales, en esa oportunidad la Sala Plena indicó que:

"(i) las leyes aprobatorias de tratados deben ser objeto de consulta previa cuando el texto afecte de forma directa a las comunidades étnicas; (ii) las medidas legislativas o administrativas que se adopten en el desarrollo del tratado que involucren directamente a una población étnica, deben someterse al proceso de consulta antes de que se presente la norma para su aprobación en el Congreso de la República; y (iii) prima facie no es necesario someter el instrumento internacional a dicho procedimiento, si éste se refiere a creación de zonas de libre comercio, sin embargo se debe hacer consulta cuando las medidas que se tomen en desarrollo del tratado afecten de forma directa a una comunidad étnica".

Con fundamento en lo anterior, la Sala concluyó que el Acuerdo de París no constituía ni contenía medidas legislativas o administrativas que afectaran de forma directa a las comunidades indígenas y afrodescendientes colombianas y, en consecuencia, su consulta previa no se tornaba obligatoria.

Una revisión del texto del Convenio sobre la Ciberdelincuencia permite concluir que las normas prescritas en él se han previsto de manera uniforme para la generalidad de los colombianos, sin que su fin sea expedir una regulación específica referida a las comunidades étnicas. Como se explicará más adelante, el objeto del presente instrumento internacional es la materialización de una política criminal común en materia de ciberdelincuencia, mediante la adopción de lineamientos establecidos en un acto jurídico con fuerza vinculante, que contiene mandatos de concreción interna para desarrollar una legislación nacional integral contra el delito cibernético en un marco de cooperación internacional entre los Estados Parte.

Estima la Sala que el Convenio sobre la Ciberdelincuencia no constituye ni contiene medidas legislativas o administrativas que afecten de forma particular a las comunidades indígenas y afrodescendientes colombianas y, en consecuencia, su consulta previa no se tornaba obligatoria. Se considera que la afectación que se puede derivar del tratado internacional bajo revisión frente a estos grupos étnicos no es distinta de la que se produce para los demás colombianos, la cual proviene del efecto general que, en principio, tienen las leyes y los tratados internacionales lo que excluye la presencia de una afectación directa.

2.3. Examen del trámite de la Ley 1928 de 2018 ante el Congreso de la República.

Como se dijo, la Constitución Política no señala un procedimiento especial para las leyes aprobatorias de los tratados internacionales y su incorporación a la legislación interna, por lo que a éstas les corresponde el trámite previsto para las leyes ordinarias, contemplado en los artículos 157, 158, 160 y 165 de la Constitución Política. Sin embargo, este trámite tiene dos particularidades, a saber: (i) por tratarse de asuntos relativos a relaciones internacionales, en virtud de lo previsto en el artículo 154 superior[27], el debate debe iniciarse en el Senado de la República, y (ii) una vez ha sido sancionada la ley por el Presidente, deberá remitirla a la Corte Constitucional dentro de los 6 días siguientes, para efectos de la revisión de constitucionalidad, según lo establecido en el numeral 10 del artículo 241 superior[28].

Con fundamento en los antecedentes legislativos, las actas publicadas en las Gacetas del Congreso de la República y las certificaciones remitidas a la Corte Constitucional por el Senado de la República y la Cámara de Representantes, esta Corporación estableció que el proyecto de ley radicado bajo los números 058 de 2017 Senado y 230 de 2018 Cámara, que finalizó con la expedición de la Ley 1928 de 2018 "Por medio de la cual se aprueba el convenio sobre la ciberdelincuencia, adoptado el 23 de noviembre de 2001, en Budapest" surtió el siguiente trámite:

2.3.1. Trámite en el Senado de la República.

El Proyecto de Ley 58 fue radicado en el Senado de la República por el Gobierno Nacional, el 1 de agosto de 2017, por la entonces Ministra de Relaciones Exteriores, María Ángela Holguín Cuéllar, el entonces Ministro de Defensa Nacional, Luis Carlos Villegas Echeverri, el entonces Ministro de Justicia y del Derecho, Enrique Gil Botero y el en ese momento Ministro de Tecnologías de la Información y las Comunicaciones David Luna.

El texto del proyecto de ley y la respectiva exposición de motivos fueron publicados en la Gaceta del Congreso N° 631 del 1 de agosto de 2017[29], cumpliéndose así, con los requisitos referentes a la iniciación de esta clase de asuntos en el Senado de la República (artículo 154 Constitucional), y la publicación del proyecto de ley antes de darle curso en la comisión respectiva (numeral 1° del artículo 157 de la Carta Política)[30].

Advertida la publicación oficial del informe de ponencia se tiene por cumplido el requisito formal de publicidad previsto en el artículo 156 de la Ley 5ª de 1992[31].

2.3.1.1. Publicación de la ponencia para primer debate:

La ponencia para primer debate fue repartida en la Comisión Segunda del Senado de la República y presentada en forma favorable por los senadores José David Name Cardozo y Jaime Durán Barrera. El texto fue publicado en la Gaceta del Congreso No. 771 del 11 de septiembre de 2017,[32] en cumplimiento del artículo 157 de la Ley 5ª de 1992[33].

2.3.1.2. Anuncio y aprobación en primer debate:

El Proyecto de Ley 58 de 2017 Senado, fue anunciado para primer debate en el Senado de la República el 12 de septiembre de 2017, tal como consta en el Acta No. 05 de esa fecha, publicada en la Gaceta del Congreso No. 1000 del 31 de octubre de 2017, en los siguientes términos:

"Siendo las 10:30 a. m. del día martes doce (12) de septiembre del año dos mil diecisiete (2017), previa convocatoria hecha por el señor Secretario de la Comisión Segunda, doctor Diego Alejandro González González se reunieron los Honorables Senadores para sesionar en la Comisión.

Control de anuncio para discusión y votación

de proyectos de ley

(…)

Proyecto de ley número 58 de 2017 Senado, por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest.

Autores: Ministra de Relaciones Exteriores, doctora María Ángela Holguín Cuéllar, Ministro de Defensa, doctor Luis Carlos Villegas Echeverri, Ministro de Justicia, doctor Enrique Gil Botero y Ministro de las Tecnologías, doctor David Luna.

Ponentes: honorables Senadores José David Name Cardozo y Jaime Durán Barrera.

Publicaciones: Texto del proyecto de ley: Gaceta del Congreso número 631 de 2017.

Ponencia Primer Debate: Gaceta del Congreso número 771 de 2017.

Están realizados los anuncios, señor Presidente"[34].

En razón a que en dicha fecha no fue aprobado, el Proyecto de Ley 58 de 2017 Senado fue anunciado nuevamente para primer debate en el Senado de la República el 19 de septiembre de 2017, tal como consta en el Acta No. 06 de esa fecha, publicada en la Gaceta del Congreso No. 1000 del 31 de octubre de 2017, en los siguientes términos:

"Siendo las 10:30 a. m. del día martes diecinueve (19) de septiembre del año dos mil diecisiete (2017), previa convocatoria realizada por el señor Secretario de la Comisión Segunda, doctor Diego Alejandro González González, se reunieron los honorables Senadores para sesionar en la Comisión.

(…)

El Secretario, doctor Diego Alejandro González González, da lectura al anuncio de proyectos de ley: Control de anuncio para discusión y votación de proyectos de ley. Por instrucciones del Presidente de la Comisión Segunda del Senado de la República, anuncio de discusión y votación de proyectos de ley para la próxima sesión de la Comisión Segunda del Senado (artículo 8° del Acto Legislativo número 1 de 2003).

Proyecto de Ley número 58 de 2017 Senado, por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest.

Autores: Ministra de Relaciones Exteriores, doctora María Ángela Holguín Cuéllar, Ministro de Defensa, doctor Luis Carlos Villegas Echeverri, Ministro de Justicia, doctor Enrique Gil Botero y Ministro de las Tecnologías, doctor David Luna.

Ponentes: honorables Senadores José David Name Cardozo y Jaime Durán Barrera.

Publicaciones: Texto del proyecto de ley: Gaceta del Congreso número 631 de 2017.

Ponencia Primer Debate: Gaceta del Congreso número 771 de 2017.

Está realizado el anuncio de proyectos de ley, señor Presidente.

El Presidente, Senador Iván Leonidas Name Vásquez:

Levanta la sesión y cita para el próximo martes a las 10:00 a. m. Termina la sesión a las 11:15 a. m".

Finalmente, el Proyecto de Ley 58 de 2017 Senado fue anunciado nuevamente para primer debate en el Senado de la República el 26 de septiembre de 2017, tal como consta en el Acta No. 07 de esa fecha, publicada en la Gaceta del Congreso No. 1184 del 12 de diciembre de 2017[35], en los siguientes términos:

"Siendo las 10:30 a. m., del día martes veintiséis (26) de septiembre del año dos mil diecisiete (2017), previa convocatoria hecha por el señor Secretario de la Comisión Segunda, doctor Diego Alejandro González González se reunieron los honorables Senadores para sesionar en la Comisión.

(…)

Discusión y votación de proyectos de ley anunciados en sesión anterior

1. Proyecto de ley número 58 de 2017 Senado, por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest.

Autor: Ministerios de: Relaciones Exteriores, Defensa Nacional, Justicia y del Derecho y Tecnologías.

Ponentes: honorables Senadores José David Name Cardozo y Jaime Durán Barrera.

Publicaciones: Proyecto de ley: Gaceta del Congreso número 631 de 2016.

Ponencia Primer Debate: Gaceta del Congreso número 771 de 2017.

(…)

El señor Secretario, doctor Diego Alejandro González González:

Me permito realizar la lectura de los anuncios para discutir y votar en la próxima sesión:

CONTROL DE ANUNCIO PARA DISCUSIÓN Y VOTACIÓN DE PROYECTOS DE LEY POR INSTRUCCIONES DEL PRESIDENTE DE LA COMISIÓN SEGUNDA DEL SENADO DE LA REPÚBLICA. ANUNCIO DE DISCUSIÓN Y VOTACIÓN DE PROYECTOS DE LEY PARA LA PRÓXIMA SESIÓN DE LA COMISIÓN SEGUNDA DEL SEMANDO (Artículo 8° DEL ACTO LEGISLATIVO NÚMERO 1 DE 2003).

-. Proyecto de ley número 58 de 2017 Senado, por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre 2001, en Budapest.

(…)

Le informo, señor Presidente, han sido anunciados los proyectos de ley para discutir y votar en la próxima sesión.

El señor Presidente, honorable Senador León Rigoberto Barón Neira:

Se levanta la sesión y se convoca para el próximo martes a las 10:10 de la mañana. La sesión finalizó siendo las 2:45 p.m.2[36].

El proyecto fue discutido y aprobado en la sesión del día 3 de octubre de 2017, según consta en el Acta No. 08 de esta fecha, publicada en la Gaceta del Congreso No. 1184 del 12 de diciembre de 2017[37], conforme al siguiente texto:

"Siendo las 10:30 a. m. del día martes tres (3) de octubre del año dos mil diecisiete (2017), previa convocatoria hecha por el señor Secretario de la Comisión Segunda, doctor Diego Alejandro González González se reunieron los honorables Senadores para sesionar en la Comisión.

(…)

Discusión y votación de proyectos de ley anunciados en sesión anterior

1. Proyecto de ley número 58 de 2017 Senado, por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest, Hungría.

Autores: Ministerios de Relaciones Exteriores, Defensa Nacional, Justicia y del Derecho y Tecnologías.

Publicaciones Texto del Proyecto de ley: Gaceta del Congreso número 631 de 2016.

Ponencia Primer Debate: Gaceta del Congreso número 771 de 2017.

(…)

El Presidente, Senador Iván Leonidas Name Vásquez: (…) sírvase leer la proposición con la cual termina la ponencia del proyecto señor Secretario.

El Secretario de la Comisión, doctor Diego Alejandro González González, informa:

Señor Presidente, honorable Senadores, la proposición con la que termina el informe de ponencia dice así: Proposición. En consecuencia y por las razones expuestas, me permito rendir ponencia positiva y le solicitamos a los honorables Miembros de la Comisión Segunda del Senado de la República, darle primer debate al Proyecto de ley número 58 de 2017, por medio de la cual se aprueba el convenio sobre la delincuencia, adoptado el 23 de noviembre de 2001, en Budapest. De los honorables Congresistas, José David Name Cardozo, Senador de la República. Jaime Durán Berrera, Senador de la República. Esta leída la proposición final señor Presidente.

El Presidente, Senador Iván Leonidas Name Vásquez:

Solicito al Secretario se sirva llamar a lista para la votación de la proposición final al proyecto de ley número 58 de 2017 Senado.

El Secretario de la Comisión, doctor Diego Alejandro González González:

Procede con el llamado a lista para la votación de la proposición final del informe de ponencia al Proyecto de ley número 58 de 2017 Senado.

Avirama Avirama Marco Aníbal

Barón Neira León Rigoberto Vota Sí.

Cepeda Castro Iván

Chamorro Cruz William Jimmy Vota Sí.

Durán Barrera Jaime Enrique

Galán Pachón Carlos Fernando

Holguín Moreno Paola Andrea Vota Sí.

Lizcano Arango Óscar Mauricio

Name Vásquez Iván Leonidas Vota Sí

Osorio Salgado Nidia Marcela Vota Sí.

Vega de Plazas Thania Vota Sí.

Velasco Chaves Luis Fernando

Le informo, señor Presidente, han votado por el SÍ, siete (7) honorables Senadores, por el NO, ninguno, en consideración ha sido aprobada la proposición final con que termina el Informe de Ponencia.

El Presidente, Senador Iván Leonidas Name Vásquez:

Solicito al Secretario se sirva leer el articulado.

El Secretario de la Comisión, doctor Diego Alejandro González González, le informo al Presidente, el Senador Jimmy Chamorro Cruz, ha solicitado la omisión de la lectura del articulado del proyecto.

El Presidente, Senador Iván Leonidas Name Vásquez:

Informa a los Senadores, está a consideración la omisión de lectura del articulado y el articulado del Proyecto de ley número 58 de 2017 Senado, lo aprueba la Comisión.

El Secretario de la Comisión, doctor Diego Alejandro González González:

Procede con el llamado a lista para la votación de la omisión de la lectura del articulado y el articulado del Proyecto de ley número 58 de 2017 Senado:

Avirama Avirama Marco Aníbal

Barón Neira León Rigoberto Vota Sí.

Cepeda Castro Iván.

Chamorro Cruz William Jimmy Vota Sí.

Durán Barrera Jaime Enrique

Galán Pachón Carlos Fernando

Holguín Moreno Paola Andrea Vota Sí.

Lizcano Arango Óscar Mauricio

Name Cardozo José David Vota Sí

Name Vásquez Iván Leonidas Vota Sí.

Osorio Salgado Nidia Marcela Vota Sí.

Vega de Plazas Thania Vota Sí.

Velasco Chaves Luis Fernando

Le informo al Presidente, han votado por el SÍ, siete (7) honorables Senadores, por el No, ninguno, en consecuencia ha sido aprobada la proposición de omisión de lectura del articulado y el articulado del Proyecto de ley número 58 de 2017 Senado.

El Presidente, Senador Iván Leonidas Name Vásquez:

Solicito al Secretario sírvase dar lectura al título del proyecto de ley número 58 de 2017.

El Secretario de la Comisión, doctor Diego Alejandro González González:

Procede con la lectura al título del Proyecto de ley número 58 de 2017, por medio del cual se aprueba el convenio sobre la ciberdelincuencia, adoptado el 23 de noviembre de 2011, en Budapest. Está leído el título señor Presidente.

El Presidente, Senador Iván Leonidas Name Vásquez:

Informa a los Senadores de la Comisión, está a consideración del proyecto. Anuncio que va a cerrarse. Lo aprueba la Comisión.

Avirama Avirama Marco Aníbal

Barón Neira León Rigoberto Vota Sí.

Cepeda Castro Iván.

Chamorro Cruz William Jimmy Vota Sí.

Durán Barrera Jaime Enrique

Galán Pachón Carlos Fernando

Holguín Moreno Paola Andrea Vota Sí.

Lizcano Arango Oscar Mauricio

Name Cardozo José David Vota Sí

Name Vásquez Iván Leonidas Vota Sí

Osorio Salgado Nidia Marcela Vota Sí.

Vega de Plazas Thania Vota Sí.

Velasco Chaves Luis Fernando

Le informo, señor Presidente, han votado por el Sí, siete (7) honorables Senadores, por el No. Ninguno, en consecuencia ha sido aprobada el título del Proyecto de ley número 58 de 2017 Senado.

El Presidente, Senador Iván Leonidas Name Vásquez:

Pregunta a los Senadores de la Comisión, quiere la Comisión que este proyecto de ley tenga segundo debate.

El Secretario de la Comisión, doctor Diego Alejandro González González:

Le informa al Presidente, los Senadores sí quieren y han aprobado que este Proyecto de ley número 58 de 2017 Senado renga su segundo debate en la Plenaria del Senado.

El Presidente, Senador Iván Leonidas Name Vásquez:

Nombra como Ponentes para el Segundo Debate a los mismos Senadores José David Name Cardozo y Jaime Enrique Durán Barrera".

El Secretario General de la Comisión Segunda Constitucional Permanente del Senado de la República, mediante certificación del 27 de agosto de 2018[38], señaló que la proposición final, la omisión de la lectura del articulado, discusión y votación del articulado propuesto, el título del proyecto y el querer que éste tenga segundo debate y se convierta en Ley de la República, fueron aprobados conforme al Acto Legislativo No. 01 de 2009, con votación nominal y pública, sin que se registraran votos en contra.

2.3.1.3. Ponencia para segundo debate

La ponencia positiva para segundo debate al proyecto de ley de la referencia fue presentada por los senadores José David Name Cardozo y Jaime Enrique Durán Barrera, según informe de ponencia en segundo debate al Proyecto de Ley 58 de 2017 Senado del 6 de octubre de 2017, publicado en la Gaceta del Congreso No. 910 del 11 de octubre de 2017[39].

2.3.1.4. Anuncio y aprobación del proyecto en segundo debate

El Proyecto de Ley 58 de 2017 Senado fue anunciado para segundo debate en el Senado de la República el 20 de marzo de 2018, como consta en el Acta No. 47 de esa fecha, publicada en la Gaceta del Congreso No. 474 del 26 de junio de 2018. El anuncio se realizó así:

“Bogotá, D. C., a los veinte (20) días del mes de marzo de dos mil dieciocho (2018) previa citación, se reunieron en el recinto del honorable Senado de la República los miembros del mismo, con el fin de sesionar en pleno.

(…)

Anuncio de proyectos

Por instrucciones de la Presidencia y, de conformidad con el Acto Legislativo 01 de 2003, por Secretaría se anuncian los proyectos que se discutirán y aprobarán en la próxima sesión.

Anuncio de proyectos de ley o de actos legislativo, que serán considerados y eventualmente votados en la sesión plenaria del honorable Senado de la República siguientes a la del día martes 20 de marzo de 2018. Dentro del trámite legislativo ordinario (negrilla agregada).

(…)

Proyecto de ley número 58 de 2017 Senado, por medio de la cual se aprueba el “Convenio sobre la Ciberdelincuencia”, adoptado el 23 de noviembre de 2001, en Budapest”[40].

Posteriormente, al no haber sido discutido en la fecha anteriormente referida, el proyecto de ley de la referencia fue anunciado nuevamente para segundo debate en el Senado de la República el 3 de abril de 2018, como consta en el Acta No. 49 de esa fecha, publicada en la Gaceta del Congreso No. 475 del 26 de junio de 2018[41] El anuncio se realizó así:

“En Bogotá, D. C., a los tres (03) días del mes de abril de dos mil dieciochos (2018) previa citación, se reunieron en el recinto del honorable Senado de la República los miembros del mismo, con el fin de sesionar en pleno.

(…)

Anuncio de proyectos

Por instrucciones de la Presidencia y, de conformidad con el Acto Legislativo 01 de 2003, por Secretaría se anuncian los proyectos que se discutirán y aprobarán en la próxima sesión.

El siguiente punto es anuncios, de proyectos de ley y de actos legislativos que serán considerados y eventualmente votados en la sesión Plenaria siguiente a la del día martes 3 de abril de 2018 del honorable Senado de la República de Colombia (negrilla agregada).

(…)

Proyecto de ley número 58 de 2017 Senado, por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest.

(…)

Están leídos todos los proyectos y esta echo el anuncio señor Presidente".

(…)

De acuerdo con la certificación expedida por el Secretario General del Senado[42], el proyecto fue aprobado en la sesión siguiente a la del 3 de abril de 2018, es decir, el 4 de abril de 2018, a través del sistema de votación nominal, con un total de 64 votos por el SI, tal y como consta en el Acta No. 50 de esa fecha, publicada en la Gaceta del Congreso No. 476 del 26 de junio de 2018.

El siguiente es el texto de la aprobación:

"La Presidencia indica a la Secretaría dar lectura a la proposición con que termina el informe.

Por Secretaría se da lectura a la proposición positiva con que termina el informe de ponencia del Proyecto de ley número 58 de 2017 Senado.

La Presidencia somete a consideración de la Plenaria la proposición positiva con que termina el Informe de ponencia del Proyecto de ley número 58 de 2017 Senado y, cerrada su discusión, abre la votación e indica a la Secretaría abrir el registro electrónico para proceder en forma nominal.

La Presidencia cierra la votación, e indica a la Secretaría cerrar el registro electrónico e informar el resultado de la votación.

Por Secretaría se informa el siguiente resultado:

Por el Sí: 64

Total: 64 Votos

Votación nominal a la proposición positiva con que termina el informe de ponencia del Proyecto de ley número 58 de 2017 Senado

por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia" adoptado el 23 de noviembre de 2001, en Budapest.

(…)

En consecuencia, ha sido aprobada la proposición positiva con que termina el informe de ponencia del Proyecto de ley número 58 de 2017 Senado.

Se abre segundo debate

Por solicitud del honorable Senador Carlos Fernando Galán Pachón, la Presidencia somete a consideración de la Plenaria la omisión de la lectura del articulado y, cierra su discusión.

La Presidencia somete a consideración de la Plenaria el articulado en bloque del proyecto y, cerrada su discusión pregunta: ¿Adopta la Plenaria el articulado propuesto?

La Presidencia indica a la Secretaría dar lectura al título del proyecto.

Por Secretaría se da lectura al título del Proyecto de ley número 58 de 2017 Senado, por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest.

Leído este, la Presidencia lo somete a consideración de la Plenaria, y cerrada su discusión pregunta: ¿Aprueban los miembros de la Corporación el título leído?

Cumplidos los trámites constitucionales, legales y reglamentarios, la Presidencia pregunta: ¿Quieren los Senadores presentes que el proyecto de ley aprobado surta su trámite en la

Honorable Cámara de Representantes?

La Presidencia abre la votación de la omisión de la lectura del articulado, el articulado en bloque, el título y que surta su trámite en la Honorable Cámara de Representantes el Proyecto de ley número 58 de 2017 Senado e indica a la Secretaría abrir el registro electrónico para proceder en forma nominal.

La Presidencia cierra la votación, e indica a la Secretaría cerrar el registro electrónico e informar el resultado de la votación.

Por Secretaría se informa el siguiente resultado:

Por el Sí: 64

Total: 64 Votos

Votación nominal a la omisión de la lectura del articulado, el articulado en bloque, título y transitorio a la otra cámara del Proyecto de ley número 58 de 2017 Senado por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest.

La Presidencia indica a la Secretaría continuar con el siguiente proyecto del Orden del Día.

(…)[43].

2.3.1.5. Publicación del texto aprobado

El texto definitivo aprobado en segundo debate en la Plenaria del Senado fue publicado en la Gaceta del Congreso No. 118 del 10 de abril de 2018[44].

2.3.2. Trámite en la Cámara de Representantes

2.3.2.1. Ponencia para primer debate:

Radicado el proyecto de ley de la referencia en la Cámara de Representantes con el número 230 de 2018, fue repartido a la Comisión Segunda Constitucional de la Cámara de

Representantes, y se designó como ponentes a los Representantes Efraín Torres Monsalvo y José Carlos Mizgher. La ponencia favorable para primer debate se encuentra publicada en la Gaceta del Congreso No. 261 del 16 de mayo de 2018[45].

2.3.2.2. Anuncio y aprobación en primer debate:

De conformidad con el texto del Acta No. 25 del 16 de mayo de 2018, publicada en la Gaceta del Congreso No. 401 del 8 de junio de 2018[46], el anuncio del proyecto de ley se realizó en los siguientes términos:

"Hace uso de la palabra el Presidente de la Comisión Segunda, honorable Representante Enfraín Antonio Torres Monsalvo:

Muy buenas tardes para todos. Señor Secretario, por favor, llame a lista.

Hace uso de la palabra el Secretario de la Comisión Segunda, doctor Benjamín Niño Flórez:

Sí, señor Presidente.

Llamado a lista, sesión Comisión Segunda, mayo 16 de 2018, siendo las 3:40 p. m.

Hace uso de la palabra el Secretario de la Comisión Segunda, doctor Benjamín Niño Flórez:

Sí, Presidente.

Con su venia, me permito primero hacer anuncios de proyectos de ley, dando cumplimiento al artículo 8° del Acto Legislativo 1 de 2003, para la próxima sesión de Comisión donde se sometan a discusión y votación proyectos de ley.

(…)

Proyecto de ley número 230 de 2018 Cámara, 058 de 2017 Senado

Han sido anunciados los proyectos de ley, Presidente.

(…)

La Comisión Segunda de la Cámara de Representantes discutió y aprobó el proyecto de ley de la referencia en la sesión del 17 de mayo de 2018, según consta en el Acta No. 26 de esa fecha, publicada en la Gaceta del Congreso No. 401 del 8 de junio de 2018[47]. Así lo certificó la Secretaria General de la Comisión Segunda Constitucional Permanente, mediante oficio del 30 de agosto de 2018:

"Certifico que en sesión de la Comisión Segunda de la Honorable Cámara de Representantes del día 17 de mayo de 2018, se le dio primer debate y se aprobó en votación nominal de acuerdo al Art. 130 de la Ley 5 de 1992 (Ley 1431 de 2011), el proyecto de ley número No. 230 de 2018 CÁMARA, 58 DE 2017 SENADO "POR MEDIO DE LA CUAL SE APRUEBA EL CONVENIO SOBRE LA CIBERDELINCUENCIA, ADOPTADO EL 23 DE NOVIEMBRE DE 2001, EN BUDAPEST", sesión a la cual asistieron 14 Honorables Representantes, en los siguientes términos:

Leída la proposición con que termina el informe de ponencia para primer debate del proyecto de ley y publicada en la Gaceta del Congreso No. 261/18, se sometió a consideración, se realiza votación nominal y pública, fue Aprobado, con trece (13) votos por el SI y ningún voto por el NO, para un total de trece (13) votos, así:

Votación

SI

NO

AGUDELO GARCÍA ANA PAOLA

BARRETO CASTILLO MIGUEL ÁNGEL

X

CABELLO FLÓREZ TATIANA

X

DELUQUE ZULETA ALFREDO RAFAEL

DURÁN CARRILLO ANTENOR

X

HOYOS SALAZAR FEDERICO EDUARDO

X

MENDOZA BUSTOS VANESSA ALEXANDRA

X

MESA BETANCUR JOSÉ IGNACIO

X

MIZGER PACHECO JOSÉ CARLOS

X

PÉREZ OYUELA JOSÉ LUIS

X

RINCÓN VERGARA NEVARDO ENEIRO

X

ROSADO ARAGÓN ÁLVARO GUSTAVO

TORRES MONSALVO EFRAÍN ANTONIO

X

TRIANA VARGAS MARÍA EUGENIA

URIBE MUÑOZ ALIRIO

X

URREGO CARVAJAL LUIS FERNANDO

X

VILLAMIZAR ORTIZ ANDRÉS FELIPE

YEPES MARTÍNEZ JAIME ARMANDO

X

Se dio lectura al articulado propuesto para primer debate del proyecto de ley publicado en la Gaceta del Congreso No. 261/18, se sometió a consideración y se aprobó en votación nominal y pública, siendo Aprobado, con trece (13) votos por el SI y ningún voto por el NO, para un total de trece (13) votos, así:

Votación

SI

NO

AGUDELO GARCÍA ANA PAOLA

BARRETO CASTILLO MIGUEL ÁNGEL

X

CABELLO FLÓREZ TATIANA

X

DELUQUE ZULETA ALFREDO RAFAEL

DURÁN CARRILLO ANTENOR

X

HOYOS SALAZAR FEDERICO EDUARDO

X

X

MESA BETANCUR JOSÉ IGNACIO

X

MIZGER PACHECO JOSÉ CARLOS

X

PÉREZ OYUELA JOSÉ LUIS

X

RINCÓN VERGARA NEVARDO ENEIRO

X

ROSADO ARAGÓN ÁLVARO GUSTAVO

TORRES MONSALVO EFRAÍN ANTONIO

X

TRIANA VARGAS MARÍA EUGENIA

URIBE MUÑOZ ALIRIO

X

URREGO CARVAJAL LUIS FERNANDO

X

VILLAMIZAR ORTIZ ANDRÉS FELIPE

YEPES MARTÍNEZ JAIME ARMANDO

X

Leído el título del proyecto de ley publicado en la Gaceta del Congreso No. 261/18 y preguntaba a la Comisión su quiere que este proyecto de ley pase a segundo debate y sea ley de la República de conformidad con el Art, 130 inciso final de la Ley 5 de 1992, se sometió a consideración y se aprobaron en votación nominal y pública, con doce (12) votos por el SI y ningún voto por el NO, para un total de doce (12) votos, así:

Votación

SI

NO

AGUDELO GARCÍA ANA PAOLA

X

CABELLO FLÓREZ TATIANA

X

DELUQUE ZULETA ALFREDO RAFAEL

DURÁN CARRILLO ANTENOR

X

HOYOS SALAZAR FEDERICO EDUARDO

X

MENDOZA BUSTOS VANESSA ALEXANDRA

X

MESA BETANCUR JOSÉ IGNACIO

X

MIZGER PACHECO JOSÉ CARLOS

X

PÉREZ OYUELA JOSÉ LUIS

X

RINCÓN VERGARA NEVARDO ENEIRO

X

ROSADO ARAGÓN ÁLVARO GUSTAVO

TORRES MONSALVO EFRAÍN ANTONIO

X

TRIANA VARGAS MARÍA EUGENIA

X

URREGO CARVAJAL LUIS FERNANDO

X

VILLAMIZAR ORTIZ ANDRÉS FELIPE

YEPES MARTÍNEZ JAIME ARMANDO

X

2.3.2.3. Ponencia para la Plenaria de la Cámara de Representantes:

La ponencia para segundo debate al proyecto de la ley de la referencia fue publicada en la Gaceta del Congreso No. 403 del 12 de junio de 2018[48], con ponencia favorable de los Representantes a la Cámara Efraín Antonio Torres Monsalvo y José Carlos Mizger Pacheco.

2.3.2.4. Anuncio y aprobación de la Plenaria:

En sesión plenaria del 19 de junio de 2018, que consta en el Acta No. 295 de esa fecha, fue anunciado el Proyecto de Ley 230 de 2018 Cámara, 58 de 2107 Senado, para la sesión del 20 de junio de 2018, en cumplimiento del artículo 8 el Acto Legislativo 01 de 2003.

Según Acta No. 296 de la sesión del 20 de junio de 2018, la Plenaria de la Cámara de Representantes aprobó el proyecto de la ley a través de votación nominal y pública, como consta en la Gaceta del Congreso 912 de 2018, información que se reiteró en la certificación expedida por el Secretario General de la Cámara de Representantes del 5 de septiembre de 2018[49].

La aprobación se realizó de la siguiente manera:[50]

"Informe con el que termina la ponencia: SI: 86 votos; NO: 0 votos.

Articulado: SI: 86 votos; No: 0 votos.

Título y pregunta: SI: 86 votos; No: 0 votos"[51].

Gaceta del Congreso 498 del 5 de julio de 2018:

"En Sesión Plenaria del día 20 de junio de 2018, fue aprobado en segundo debate el texto definitivo sin modificaciones al Proyecto de ley número 230 de 2018 Cámara, 58 de 2017 Senado, por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest. Esto con el fin de que el citado proyecto de ley siga su curso legal y reglamentario y de esta manera dar cumplimiento con

lo establecido en el artículo 182 de la Ley 5ª de 1992.

TEXTO DEFINITIVO PLENARIA CÁMARA AL PROYECTO DE LEY NÚMERO 230 DE 2018 CÁMARA, 58 DE 2017 SENADO

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

DECRETA:

Artículo 1°. Apruébase el Convenio sobre la Ciberdelincuencia, adoptado el 23 de noviembre de 2001, en Budapest.

Artículo 2°. 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 3°. La presente ley rige a partir de la fecha de su publicación".

(…)

"En Sesión Plenaria del día 20 de junio de 2018, fue aprobado en segundo debate el texto definitivo sin modificaciones al Proyecto de ley número 230 de 2018 Cámara, 58 de 2017 Senado, por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest. Esto con el fin de que el citado proyecto de ley siga su curso legal y reglamentario y de esta manera dar cumplimiento con lo establecido en el artículo 182 de la Ley 5ª de 1992.

Lo anterior, según consta en las actas de Sesión Plenaria número 296 de junio 20 de 2018, previo su anuncio en la Sesión del día 19 de junio de los corrientes, correspondiente al Acta número 295"[52].

2.3.2.5 Sanción Presidencial y envío a la Corte Constitucional

El 24 de julio de 2018, la Ministra de Educación, delegataria de funciones presidenciales mediante Decreto 1255 del 19 de julio de 2018, sancionó la Ley 1928 de 2018, por medio de la cual se aprueba el instrumento internacional que es objeto de estudio[53].

Lo anterior, de conformidad con las facultades que le confiere el artículo 196 de la Constitución Política al Presidente de la República para delegar funciones constitucionales en su ausencia por motivos del cargo, previa verificación del cumplimiento de las disposiciones establecidas en la Constitución Política.

Posteriormente, el 30 de julio de 2018, fue remitido el texto de la ley por la Secretaría Jurídica de la Presidencia de la República a la Corte Constitucional, dando cumplimiento al término de seis días otorgado por el numeral 10 del artículo 241 de la Constitución[54].

2.4. CONSTITUCIONALIDAD DEL TRÁMITE DADO A LA LEY 1928 de 2018

Luego del recuento anterior, pasa la Corte a determinar la constitucionalidad del trámite de aprobación de la Ley 1928 de 2018.

2.4.1. Oportunidad en la radicación del proyecto de ley en el Senado de la República

La Corte observa que la Aprobación Ejecutiva del Convenio fue suscrita por el Presidente de la República el día 8 de junio de 2017[55]. Por otro lado, se verifica que la radicación del proyecto de ley en el Senado de la República por parte de los Ministros de Relaciones Exteriores, de Defensa Nacional, de Justicia y del Derecho y de Tecnologías de la Información y las Comunicaciones, se realizó 1 de agosto de 2017, según consta en la Gaceta del Congreso No. 631 de esa fecha[56].

De esta manera, se dio cumplimiento a los requisitos referentes a la iniciación de esta clase de asuntos en el Senado de la República (artículo 154 Constitucional).

2.4.2. Oportunidad de la publicación del proyecto de ley y cumplimiento de los requisitos del artículo 157 superior

El artículo 157, numeral 1 de la Constitución Política establece que ningún proyecto será ley sin "[h]aber sido publicado oficialmente por el Congreso, antes de darle curso en la comisión respectiva". Sobre el particular, esta Corte constata el cumplimiento de este

requisito, pues el mismo fue publicado el 1 de agosto de 2017[57] y se inició el trámite en la Comisión Segunda del Senado el 11 de septiembre de 2017[58].

Además, fue aprobado en primer debate en las correspondientes comisiones de cada cámara[59], aprobado en segundo debate en las plenarias de cada cámara[60] y recibió la debida sanción presidencia[61].

2.4.3. Cumplimiento del primer inciso del artículo 160 superior

Entre el primer y segundo debate en cada una de las cámaras transcurrió un tiempo no inferior a ocho días, tal como lo ordena el artículo 160 Constitucional: la aprobación en primer debate en la Comisión Segunda del Senado tuvo lugar el 3 de octubre de 2017[62], mientras que la aprobación en la plenaria ocurrió el 4 de abril de 2018[63]; del mismo modo, la aprobación en primer debate en la Comisión Segunda de la Cámara ocurrió el 17 de mayo de 2018[64], y el segundo debate tuvo lugar el 20 de junio de 2018[65].

De otro lado, entre la aprobación del proyecto en el Senado (4 de abril de 2018) y la iniciación del debate en la Cámara de Representantes (17 de mayo de 2018) transcurrió un lapso no inferior a quince días, en cumplimiento del artículo 160 de la Carta Política.

2.4.4. Cumplimiento del quórum decisorio.

El proyecto fue discutido y aprobado en cuatro debates, en Comisiones y Plenarias de ambas Cámaras, de acuerdo con lo dispuesto en el artículo 157 superior.

Tratándose de la aprobación del proyecto en cada uno de los debates adelantados por las mayorías exigidas, la Corte constata que en las certificaciones remitidas por el Congreso de la República y en las actas y gacetas, se acredita el cumplimiento de este requisito y se deja consignado que la votación fue nominal y pública.

Es necesario tener en cuenta que, de conformidad con el artículo 5º del Acto Legislativo No. 01 de 2009, que reformó el artículo 133 de la Constitución, en los cuerpos colegiados de elección directa, el voto de sus miembros "será nominal y público, excepto en los casos que determine la ley", de donde se desprende que en el trámite legislativo la votación nominal y pública es la regla general, que ha sido exceptuada mediante la Ley 1431 de 2011, "por la cual se establecen las excepciones a que se refiere el artículo 133 de la Constitución

Política".

2.4.5. Cumplimiento del requisito de anuncio del artículo 160 constitucional, tal como fue modificado por el artículo 8º del Acto Legislativo 01 de 2003

En cuanto al cumplimiento del requisito del anuncio de que trata el artículo 8° del Acto Legislativo 01 de 2003[66], que adicionó el artículo 160 de la Constitución Política, encuentra la Corte que dicho requisito también se cumplió.

En efecto, el artículo 8º del Acto Legislativo 01 de 2003 dispone lo siguiente:

"Ningún proyecto de ley será sometido a votación en sesión diferente a aquella que previamente se haya anunciado. El aviso de que un proyecto será sometido a votación lo dará la presidencia de cada cámara o comisión en sesión distinta a aquella en la cual se realizará la votación."

Según lo establece la jurisprudencia pertinente, esta disposición busca evitar la votación sorpresiva de los proyectos de ley y actos legislativos, en aras de permitir que los congresistas se enteren de los proyectos que van a ser discutidos y votados en las sesiones siguientes.[67] Según la Corte, la finalidad del anuncio es la de"permitir a los Congresistas saber con anterioridad cuales proyectos de ley o informes de objeciones presidenciales serán sometidos a votación, suponiendo el conocimiento pleno de los mismos y evitando, por ende, que sean sorprendidos con votaciones intempestivas".[68]

La exigencia del anuncio previo es entonces de rango constitucional, para afianzar el principio democrático, el respeto por las minorías parlamentarias, y la publicidad y transparencia del proceso legislativo.

Ahora bien, del texto de la disposición constitucional se desprende que el anuncio debe cumplir los siguientes requisitos:[69]

"a) El anuncio debe estar presente en la votación de todo proyecto de ley.

b) El anuncio debe darlo la presidencia de la cámara o de la comisión en una sesión distinta y previa a aquella en que debe realizarse la votación del proyecto.

c) La fecha de la votación debe ser cierta, es decir, determinada o, por lo menos, determinable.

d) Un proyecto de ley no puede votarse en una sesión distinta a aquella para la cual ha sido anunciado".

En el caso concreto de la aprobación del proyecto de la Ley 1928 de 2018, esta Corporación encuentra lo siguiente:

En el curso del proyecto durante su primer debate en la Comisión Segunda del Senado, en tres ocasiones diferentes se realizó el anuncio del proyecto para la próxima sesión de la Comisión: primer anuncio el 12 de septiembre de 2017 (Acta No. 05, publicada en la Gaceta del Congreso No. 1000 del 31 de octubre de 2017), segundo anuncio el 19 de septiembre de 2017 (Acta No. 06, publicada en la Gaceta del Congreso No. 1000 del 31 de octubre de 2017) y tercer anuncio el 26 de septiembre de 2017 (Acta No. 07, publicada en la Gaceta del Congreso No. 1184 del 12 de diciembre de 2017).

El proyecto fue discutido en la sesión que se llevó a cabo el 3 de octubre de 2017 y en donde se aprobó el proyecto de ley número 58 de 2017 Senado (Acta No. 08, publicada en la Gaceta del Congreso No. 1184 del 12 de diciembre de 2017).

Sobre la secuencia de anuncios en la Plenaria del Senado se debe precisar que el anuncio del proyecto se realizó según consta en las Actas 47 del 20 de marzo de 2018 y 49 del 3 de abril de la misma anualidad; particularmente, se resalta que existió anuncio del proyecto de ley en la sesión inmediatamente anterior a la de su aprobación en el Senado de la República, la cual se efectúo el 4 de abril de 2018. Así, tanto para los congresistas de la correspondiente cámara legislativa, como para los ciudadanos interesados en la formación de esta ley, la fecha en que se haría la votación del proyecto era claramente determinable y futura, lo cual asegura que los fines de este requisito constitucional se cumplieron a cabalidad.

Igualmente, en el trámite del segundo debate en la plenaria del Senado, el proyecto se anunció para la próxima sesión en dos ocasiones: el 20 de marzo de 2018 (Acta No. 47, publicada en la Gaceta del Congreso No. 474 del 26 de junio de 2018); no obstante, no fue aprobado en ninguna de las sesiones siguientes a esa fecha, razón por la cual, se anunció

nuevamente el 3 de abril de 2018 para la sesión siguientes, la cual se realizó el 4 de abril de 2018 (Acta No. 49, publicada en la Gaceta del Congreso No. 475 del 26 de junio de 2018). El proyecto se aprobó el 4 de abril de 2018, publicado en la Gaceta del Congreso No. 118 del 10 de abril de 2018.

Por su parte, en cuanto a lo ocurrido en la Cámara de Representantes, se encontró que el anuncio para primer debate se realizó el 16 de mayo de 2018 (Acta No. 25 de esa fecha, publicada en la Gaceta del Congreso No. 401 del 08 de junio de 2018) para la próxima sesión, la que se realizó el 17 de mayo

de 2018, donde se discutió y aprobó el proyecto (Acta No. 26, publicada en la Gaceta del Congreso No. 401 del 12 de junio de 2018).

Finalmente, en el segundo debate en la Plenaria de la Cámara de Representantes, el proyecto de ley se anunció el 19 de junio de 2018 (Acta No. 295 de esa fecha, publicada en la Gaceta del Congreso No. 981 del 14 de noviembre de 2018[70]) para el 20 de junio de 2018, fecha en la que el proyecto fue aprobado (Acta No. 296 de esa fecha, publicada en la Gaceta del Congreso No. 912 del 29 de octubre de 2018[71]).

2.4.6. Cumplimiento del artículo 162 de la Constitución.

El artículo 162 de la Constitución Política señala que "Los proyectos de ley que no hubieren completado su trámite en una legislatura y que hubieren recibido primer debate en alguna de las Cámaras, continuarán su curso en la siguiente, en el estado en que se encuentren. Ningún proyecto de ley podrá ser considerado en más de dos legislaturas". (Subrayado fuera de texto)

Observa la Corte que se le dio cabal cumplimiento a lo preceptuado en el artículo 162 superior. Lo anterior, se verifica al observar la fecha en que el proyecto fue radicado en el Senado de la República y la fecha en que fue aprobado en cuarto debate. Así, el proyecto fue radicado en el Senado de la República el 1 de agosto de 2017, es decir, en la legislatura que empezó el 20 de julio de 2017 y que terminó el 20 de junio de 2018. Por su parte, el proyecto fue aprobado por la Plenaria de la Cámara de Representantes el 20 de junio de 2018, es decir, se dio dentro de la misma legislatura.

En consecuencia, colige la Corte Constitucional que desde el punto de vista formal, la Ley 1928 de 2018 cumplió el procedimiento legislativo previsto en la Constitución Política de Colombia y en la Ley 5 de 1992[72].

Concluido el análisis de forma del procedimiento de aprobación del proyecto de la ley de la referencia, procede la Corte a realizar el estudio material del Convenio objeto de revisión.

3. El contenido material de la Ley 1928 de 2018 y la constitucionalidad del CONVENIO SOBRE LA CIBERDELINCUENCIA.

3.1. El Convenio sobre la Ciberdelincuencia

El Convenio de Budapest es un acuerdo internacional para combatir el crimen organizado transnacional, específicamente los delitos informáticos, cuyo objetivo es establecer una legislación penal y procedimientos comunes entre sus Estados Parte que proteja a la sociedad frente a la ciberdelincuencia.

El citado Convenio fue adoptado el 8 de noviembre de 2001, durante la Sesión No. 109 del Comité de Ministros del Consejo de Europa, y se presentó para su firma en la ciudad de Budapest el 23 de noviembre de la referida anualidad; entró en vigencia el 1 de julio de 2004[73].

Este acuerdo tiene como objetivo establecer una política penal común para proteger a la comunidad internacional frente a la cibercriminalidad, mediante la creación de nuevos mecanismos de cooperación transnacional frente a los delitos cibernéticos.

La necesidad de combatir las amenazas cibernéticas implica otorgarle a los Estados signatarios del Convenio la facultad de, en términos de su preámbulo, "detectar, investigar y sancionar" aquellas conductas que constituyen actos que ponen en peligro los sistemas, redes y datos informáticos, con el fin de "proteger los intereses legítimos en la utilización y el desarrollo de las tecnologías de la información".

El Convenio pretende que los Estados puedan perseguir a los "ciberdelincuentes" mediante la implementación de nuevos tipos penales, así como el establecimiento de facultades de investigación más robustas. Su articulado se divide en cuatro capítulos (artículos 1 a 48), en los cuales se clasifican los siguientes delitos[75]:

· Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos.

· Delitos informáticos.

· Delitos relacionados con el contenido.

· Delitos relacionados con infracciones a la propiedad intelectual y de los derechos afines.

· Otras formas de responsabilidad y de sanciones.

Asimismo, el Convenio dispone que cada Parte deberá adoptar medidas legislativas para tipificar como delito en su derecho interno los actos descritos en el cuerpo del Tratado analizado.

Finalmente, el Convenio sobre la Ciberdelincuencia señala que se deben establecer sanciones a aplicar en cada caso, incluyendo las figuras de tentativa y complicidad en los delitos señalados en el artículo 11 del referido instrumento internacional. Adicionalmente, se aclara que las sanciones deben ser efectivas, proporcionadas y disuasorias, aun cuando se trate de penas privativas de la libertad (artículo 13).

3.2. Disposiciones específicas del Convenio sobre la Ciberdelincuencia

3.2.1. Preámbulo: objetivo y necesidad

De conformidad con el preámbulo, los Estados miembros del Consejo de Europa y los demás Estados signatarios del Convenio sobre la Ciberdelincuencia persiguen el objetivo de establecer una política penal para resguardar a la comunidad internacional frente a la cibercriminalidad. Específicamente, se pretende proteger los intereses legítimos en la utilización y el desarrollo de las tecnologías de la información, mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional.

Conscientes de los profundos cambios provocados por la digitalización, la convergencia y la globalización continua de las redes informáticas, los miembros del Consejo de Europa consideran necesario el Convenio para “prevenir los actos que pongan en peligro la

confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistemas redes y datos, garantizando la tipificación como delito de dichos actos"[76].

En el cuerpo del preámbulo del instrumento internacional objeto de análisis constitucional, se señala como puntos de partida para la elaboración del Tratado, entre otros: (i) el Convenio de 1981 del Consejo de Europa para la protección de las personas con respecto al tratamiento informatizado de datos personalizados; (ii) la Convención sobre los Derechos del Niño de las Naciones Unidas (1989) y el Convenio sobre las peores formas de trabajo infantil de la Organización Internacional del Trabajo; (iii) las Recomendaciones del Comité de Ministro No. R (85) 10 relativas 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 (82) 2 sobre medidas encaminadas a luchar contra la piratería en materia de propiedad intelectual y derechos afines, No. R (95) 4 sobre la protección de los datos personales en el ámbito de los servicios de telecomunicaciones, No. R (89) 9 sobre delincuencia relacionada con la informática, que ofrece a los legisladores nacionales directrices para definir ciertos delitos informáticos, y No. R (95) 13 relativa a los problemas de procedimiento penal vinculados a la tecnología de la información; (iv) la Resolución No. 1 adoptada por los Ministros de Justicia Europeos[77] para apoyar las actividades en relación con la ciberdelincuencia organizadas por el Comité Europeo para Problemas Criminales (CDPC); (v) la Resolución No. 3 que exhorta a las partes a encontrar soluciones que permitan al mayor número posible de Estados ser parte en el Convenio[78]; y, (vi) el plan de acción adoptado por los Jefes de Estado y de gobierno del Consejo de Europa[79], con el objeto de encontrar respuestas comunes ante el desarrollo de las nuevas tecnologías de la información, basadas en las normas y los valores de ese órgano.

Finalmente, en el preámbulo del Convenio sobre la Ciberdelincuencia se aclara que en su elaboración se tuvieron en cuenta los convenios existentes del Consejo de Europa sobre cooperación en materia penal, así como otros tratados similares celebrados entre los Estados miembros de ese órgano y otros Estados. Lo anterior, con el fin de mejorar las acciones organizadas por las Naciones Unidas, la OCDE, la Unión Europea y el G8.

La Corte encuentra que los principios y objetivos planteados en el preámbulo del Convenio sobre la Ciberdelincuencia no contradicen la Constitución Política de 1991, pues su interés

principal es establecer una política penal para resguardar a la comunidad internacional frente a la cibercriminalidad. No obstante, se aclara que las remisiones a instrumentos internacionales propios del espacio europeo relacionados en el cuerpo del referido preámbulo no surtirán ningún efecto vinculante, por cuanto no han sido ratificados por Colombia. Asimismo, el artículo 39 del Convenido Sobre la Ciberdelincuencia indica que los Estados Parte podrán celebrar a futuro acuerdos sobre las materias reguladas en los instrumentos internacionales citados en el presente Convenio; en esa medida se aclara que, los mismos deberán someterse al trámite de constitucionalidad dispuesto para los tratados.

3.2.2. Constitucionalidad de las normas contenidas en el Capítulo I

Terminología

Definiciones (artículo 1). Este acápite establece una serie de definiciones para efectos del Convenio, las cuales permiten fijar el contenido del mismo. En este apartado se determinan los conceptos más importantes en que se funda, tales como "sistema informativo", "datos informáticos", "proveedores de servicios" y "datos sobre el tráfico".

Encuentra la Sala Plena que la referida terminología resulta necesaria para la homogénea interpretación por parte de los Estados signatarios del Convenio. En esa medida, las disposiciones contenidas en dicho instrumento a modo de explicación de los conceptos técnicos más empleados en su articulado no desconocen norma alguna de la Constitución Política; por el contrario, guardan armonía con los artículos 15, 226 y 227 superiores.

3.2.3. Constitucionalidad de las normas contenidas en el Capítulo II

Medidas que deberán adoptarse a nivel nacional

Sección 1 (artículos 2 al 13). Derecho penal sustantivo

El Convenio sobre la Ciberdelincuencia se establece con el objeto de construir una Política criminal común, encaminada a sancionar los delitos cometidos en el ciberespacio, mediante la adopción de medidas legislativas en el derecho interno colombiano en armonía con los artículos 2 a 12 del referido Tratado.

La sección 1 del instrumento comprende los siguientes títulos: 1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informativos (arts. 2, 3, 4, 5 y 6); 2. Delitos informáticos (arts. 7 y 8); 3. Delitos relacionados con el contenido (art. 9); 4. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines (art. 10); 5. Otras formas de responsabilidad y de sanciones (arts. 11, 12 y 13).

Para el desarrollo del anterior articulado, el Convenio sobre la Ciberdelincuencia dispone que cada Parte deberá adoptar las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las conductas referidas, con el fin de poder endilgarse responsabilidad a las personas naturales y si el Estado parte así lo dispone a las personas jurídicas por los delitos previstos y garantizar la imposición de sanciones o medidas penales o no penales efectivas, proporcionadas y disuasorias, incluidas multas pecuniarias a quien se hallen responsables.

Título 1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos (arts. 2, 3, 4, 5 y 6)

En este acápite se identifica una serie de herramientas de derecho penal sustantivo propuestas en el Convenio que obliga a las Partes a tipificar delitos propiamente informáticos (como el acceso ilícito a un sistema informático, la interceptación ilícita, la interferencia en los datos o de daño informático).

La Universidad Sergio Arboleda, en intervención presentada en el proceso de la referencia, solicitó a esta Corporación formular reserva en los términos del numeral 2 del artículo 4 del Convenio que estipula: “cualquier Parte podrá reservarse el derecho a exigir que los actos definidos en el apartado 1[80] provoquen daños graves”. Lo anterior, al argumentar la necesidad de intervención del derecho penal como última ratio.

La Corte encuentra que tal petición no está llamada a prosperar pues aun cuando no hay duda de que el principio de última ratio constituye un límite esencial al poder punitivo del Estado, la decisión de intervenir penalmente es del legislador; así como su capacidad para consagrar tipos penales de peligro, si lo estima necesario. Además, la Corte observa que muchos de los tipos penales descritos en el Tratado se encuentran en el derecho interno. De igual manera, la ley podrá ser sujeta a control de constitucionalidad caso a caso.

Título 2. Delitos informáticos (arts. 7 y 8)

El Convenio tipifica la falsificación informática y el fraude informático como actos deliberados ejecutados con la intención delictiva de obtener ilegítimamente un beneficio económico propio o para un tercero y que causan un perjuicio patrimonial a una persona.

Título 3. Delitos relacionados con el contenido (art. 9)

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 delitos relacionados con el contenido como la pornografía infantil y cualquier conducta tendiente a promover su oferta, difusión, transmisión, posesión o adquisición por medios informáticos.

Título 4. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines (art. 10)

Se deberán tipificar en el derecho interno las infracciones de la propiedad intelectual, según se definan en la legislación del Estado parte y de conformidad con las obligaciones asumidas en aplicación del Acta de París del 24 de julio de 1971.

Título 5. Otras formas de responsabilidad y de sanciones (arts. 11, 12 y 13).

Encuentra la Corte que las disposiciones contenidas en este acápite no contrarían los principios ni desconocen los derechos constitucionales de nuestro ordenamiento, pues los delitos tipificados en el Convenio sobre la Ciberdelincuencia se subordinan a las regulaciones del derecho interno y a la adopción de los tipos y sanciones acordados en los instrumentos internacionales.

La configuración de los delitos consagrados en los artículos 2 al 12 del Tratado apunta a la protección de bienes jurídicos de relevancia constitucional; en particular, se pretende garantizar la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos. Lo anterior, se compagina con el amplio desarrollo jurisprudencial que esta Corporación ha proferido sobre el tema. Sin embargo, la declaratoria de constitucionalidad de la posibilidad de tipificar los delitos realizada por la Corte en los referidos artículos no obsta para que, cuando efectivamente se defina como delito alguna de las conductas de

que tratan los citados preceptos, esta Corporación revise si la norma se ajusta a la Constitución, por cualquiera de los mecanismos de control constitucional previstos en la Constitución Política.

La Corte Constitucional en la Sentencia C-748 de 2011 estudió la constitucionalidad de la Ley Estatutaria 1581 de 2012, "por la cual se dictan disposiciones generales para la protección de datos personales", norma general que establece los principios a los que está sujeto cualquier tipo de tratamiento de datos en Colombia. En esa oportunidad, resaltó que la ley estatutaria de habeas data de 2012 establece como pilares normativos los de legalidad, finalidad, libertad, veracidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad. No obstante, aclaró que tales principios "no obstan para que en el proceso de administración de bases de datos se dé aplicación a los principios rectores derivados directamente de la Constitución al igual que a aquellos derivados del núcleo temático del proyecto de ley estatutaria, los cuales pese a no encontrase numerados se entiende (sic) incorporados en razón de una lectura sistemática del proyecto de Ley Estatutaria"[81].

Para esta Corporación, el deber de adopción en el derecho interno de los requerimientos contenidos en la sección 1 del Capítulo II del Tratado objeto de revisión preserva el principio de legalidad; en esa medida, debe entenderse que el mandato de tipificación como delito de las conductas ahí descritas parte del respeto por la autonomía normativa estatal, sujeta a un esquema de responsabilidad subjetiva y admisible en el derecho penal colombiano. No obstante, la declaratoria de exequibilidad de la referida sección o de la totalidad del Convenio sobre la Ciiberdelincuencia en ningún caso implicará la elusión del control abstracto de constitucionalidad de las normas que lo desarrollen.

Las medidas que deberán adoptarse a nivel nacional en la legislación sustantiva persiguen la protección de los datos personales en un mundo globalizado en el que el poder informático es creciente. Esta protección responde a la importancia que tales datos revisten para la garantía de otros derechos como la intimidad, el buen nombre y el libre desarrollo de la personalidad.

Así, los delitos señalados en los títulos 1 y 2 se adecuan a lo establecido en la Ley 1273 de 2009, "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, entre otras disposiciones". No obstante, las medidas que se adopten en la legislación sustantiva a nivel nacional estarán sometidas a los controles de constitucionalidad que consagra la Constitución Política de 1991.

Los delitos considerados en el título 3 (relacionados con el contenido) guardan plena consonancia con la prevalencia del interés superior de los niños, las niñas y los adolescentes y de la protección de sus derechos (artículo 44 C.P), así como la total prohibición de la deliberada e ilegítima producción, oferta, difusión o posesión de pornografía infantil.

El concepto de "pornografía infantil" estatuido para los efectos del Convenio, no se restringe al material que contenga la representación visual de menores de 18 años, pues incorpora la definición de que trata el artículo 2 del Protocolo Facultativo de la Convención sobre los Derechos del Niño relativo a la Venta de Niños, la Prostitución Infantil y la Utilización de los Niños en la Pornografía[82], adoptado en Nueva York, el veinticinco (25) de Mayo de dos mil (2000), aprobado por la Ley 765 de 2002, declarada exequible por esta Corporación en Sentencia C-318 de 2003. En ese contexto, concuerda no solo con la legislación penal colombiana, sino de manera especial, con las disposiciones contendidas en la Constitución Política de 1991 y con las incorporadas como parte del bloque de constitucionalidad.

Sobre los delitos relacionados con el contenido, específicamente con la pornografía infantil, la Universidad Sergio Arboleda solicitó a la Corte Constitucional realizar una reserva frente al artículo 9, literales b y c, en los términos del numeral 4 de la referida norma del Convenio. Lo anterior, al afirmar que "el concepto de pornografía infantil debe limitarse a las representaciones visuales de menores comportándose de una forma sexual explícita (es decir, a las fotos o grabaciones) y no debe ampliarse a otras representaciones en donde personas que parecen menores de edad realizan actividades sexuales; o a imágenes realistas que representan a menores comportándose de la misma manera (dibujos grabados, esculturas, etc.)".

Para esta Corporación no existe la necesidad de formular reserva en los términos

planteados por la interviniente, pues la norma cuestionada se ajusta al derecho interno, a la Constitución Política de 1991 y al Protocolo Facultativo Sobre los Derechos del Niño Relativo a la Venta de Niños, la Prostitución Infantil y la Utilización de los Niños en la Pornografía.

Específicamente, el literal c del artículo 2 del citado instrumento internacional consagra: "por pornografía infantil se entiende toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explicitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales" (negrilla agregada).

Asimismo, el artículo 11 de Protocolo preceptúa:

"ARTÍCULO 11: Nada de lo dispuesto en el presente Protocolo se entenderá en perjuicio de cualquier disposición más propicia a la realización de los derechos del niño que esté contenida en: a) La legislación de un Estado Parte; b) El derecho internacional en vigor con respecto a ese Estado" (negrilla agregada).

La Sala Plena concluye que es constitucionalmente válido que también la representación de una persona que parece un menor de edad (pero que no lo es), adoptando un comportamiento sexualmente explícito, pueda ser considerada pornografía infantil, pues lo que se pretende es la protección del niño al evitar que este tipo de "representaciones" fomenten directamente la explotación sexual, la venta, la prostitución y la utilización de niños en la pornografía en la internet y en otros medios tecnológicos.

El título 4 del Convenio, Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines, concuerda con los preceptos incorporados de forma autónoma por el legislador colombiano en el Título VIII del Código Penal (De los delitos contra los derechos de autor), en desarrollo del mandato del artículo 61 de la C.P[83].

Esta Corporación en Sentencia C-148 de 2015 indicó que la propiedad intelectual comprende: "(i) la propiedad industrial, que preserva en general lo relativo a marcas y patentes, y (ii) los derechos de autor y conexos, que buscan salvaguardar las obras literarias, científicas y artísticas y amparar igualmente los derechos de artistas, intérpretes, ejecutantes, y productores de fonogramas, así como los de los organismos de radiodifusión, respecto de su emisión".

En esa oportunidad, se refirió a la doble dimensión jurídica de los derechos de autor, entendida como: "(i) El derecho moral, es inalienable, irrenunciable, extrapatrimonial y perpetuo. Se refiere a la posibilidad de que el autor de determinada creación, reivindique en cualquier momento la paternidad de su obra, exigiendo que se indique su nombre o seudónimo cuando esta se haga pública por cualquier medio. Comprende igualmente el derecho a oponerse a cualquier deformación, mutilación o modificación de su obra que desconozca su reputación, así como a la posibilidad de mantenerla inédita o anónima, o modificarla antes o después de hacerla pública" y "(ii) Los derechos patrimoniales de autor, por otra parte, tienen que ver con la facultad del autor de una creación, de disponer de su obra. Ello implica, la posibilidad de cederla, transferirla, renunciar a ella, etc. De acuerdo con la definición de la Organización Mundial de la Propiedad Intelectual, estos derechos implican que "el titular del derecho de autor puede hacer toda clase de utilizaciones públicas de la obra previo abono de una remuneración"[84].

En relación con las otras formas de responsabilidad como la tentativa y complicidad contenidas en el artículo 11, título 5, sección 1 del capítulo II, se observa que son figuras que se ajustan al ordenamiento interno comoquiera que pretenden dar una respuesta adecuada a conductas delictivas de menor grado de compromiso o responsabilidad, y de menor nivel de desarrollo y daño; asimismo, han sido analizadas por el legislador ampliamente.

El artículo 27 de la Ley 599 de 2000, Código Penal colombiano, determina como tentativa: "El que iniciare la ejecución de una conducta punible mediante actos idóneos e inequívocamente dirigidos a su consumación, y ésta no se produjere por circunstancias ajenas a su voluntad, (…)".

Por su parte, la figura del cómplice, está definida en el artículo 30 del cuerpo normativo referido (Participes) de la siguiente forma: "quien contribuya a la realización de la conducta antijurídica o preste una ayuda posterior, por concierto previo o concomitante a la misma, incurrirá en la pena prevista para la correspondiente infracción disminuida de una sexta parte a la mitad".

La Corte en la Sentencia C-015 de 2018 concluyó que cómplice es quien "presta una ayuda o brinda un apoyo para la realización de la conducta ilícita, sin que dicha participación sea

esencial para la ejecución típica, es decir, participa sin tener el dominio del hecho". En esa oportunidad la Sala Plena reiteró la Sentencia del 12 de septiembre del 2002, Rad. 1740 proferida por la Corte Suprema de Justicia sobre la figura de la complicidad, a saber:

"(…) Basta, sin embargo, para despejar el equívoco y dejar en claro la objetividad legal de la distinción, precisar, en uno y otro caso, si el actor se halla ligado finalísticamente o no a la realización de la conducta. En la primera hipótesis, cuando brinda colaboración posterior a un hecho punible del cual hace parte, por razón de su compromiso objetivo y subjetivo con sus resultados, se trata de un coautor. Pero si esa ayuda es de mera coadyuvancia externa a los fines de los integrantes de la empresa común, despojada de alianza anímica con los propósitos últimos de sus autores directos, quien así actúa es cómplice del hecho punible. \ De acuerdo con esta última conclusión, que hoy reitera la Sala, bastará conjugar elementos objetivos y subjetivos en la consumación de la conducta, para diferenciar la coautoría y la complicidad, en la medida en que para que una persona pueda ser considerada coautora de un delito, no sólo se exige su voluntad incondicional de realizarlo, sino también su contribución objetiva, es decir, la importancia de su aporte en la fase ejecutiva, pues ello es lo que en últimas determina el llamado "codominio del hecho", entendiendo como "hecho" el proceso causal que con la conducta se pone en marcha".

De lo anterior, la Sala concluye que no existen reparos de constitucionalidad frente al artículo 11 del Título 5, Sección 1 del Capítulo II del Convenio sobre la Ciberdelincuencia, pues respeta los principios constitucionales y se ajusta a los intereses del ordenamiento penal. No obstante, las medidas que se adopten en la legislación sustantiva a nivel nacional deberán respetar los límites constitucionales y podrán someterse al control de constitucionalidad por parte de esta Corporación, a través de los mecanismos establecidos en la Constitución Política.

Sobre la previsión relativa a la responsabilidad penal de las personas jurídicas por delitos de que trata el artículo 12 del Convenio, se observa que esta disposición no encuentra oposición constitucional alguna, pues encuentra sustento en el artículo 250 de la C.P. al existir un deber en cabeza de la Fiscalía General de la Nación de investigar y perseguir hechos que revistan las características de un delito, sin que exista una limitación constitucional sobre la naturaleza de las personas.

La Corte Constitucional en la Sentencia C-320 de 1998 se pronunció sobre la imputación penal que se proyecte sobre las personas jurídicas: “las sanciones a ser aplicadas a las personas jurídicas serán aquéllas susceptibles de ser impuestas a este tipo de sujetos y siempre que ello lo reclame la defensa del interés protegido. En este sentido, la norma examinada se refiere a las sanciones pecuniarias, a la cancelación del registro mercantil, a la suspensión temporal o definitiva de la obra y al cierre temporal o definitivo del establecimiento o de sus instalaciones. Esta clase de sanciones – que recaen sobre el factor dinámico de la empresa, su patrimonio o su actividad – se aviene a la naturaleza de la persona jurídica y, en modo alguno, resulta contraria a las funciones de la pena. La determinación de situaciones en las que la imputación penal se proyecte sobre la persona jurídica, no encuentra en la Constitución Política barrera infranqueable; máxime si de lo que se trata es de avanzar en términos de justicia y de mejorar los instrumentos de defensa colectiva”. (Negrilla agregadas).

La Sala Tercera de Revisión de esta Corporación en Sentencia T-909 de 2011 se pronunció sobre la responsabilidad de las personas jurídicas e indicó que sufren las consecuencias de los actos o hechos de las personas naturales que puedan causar un daño. Aclaró que, en los términos del art. 2341 del Código Civil, su responsabilidad puede ser directa; es decir, “por el hecho propio” o indirecta “por el hecho de otro”, según el inciso primero del artículo 2347 de la misma norma. Lo anterior, al reiterar que “toda persona es responsable, no solo de sus propias acciones para el efecto de indemnizar el daño, sino del hecho de aquellos que estuvieron a su cuidado”[85].

En esa oportunidad, la Corte abordó el desarrollo jurisprudencial que la Sala de Casación Civil de la Corte Suprema de Justicia ha realizado de estas dos modalidades y concluyó que en materia de responsabilidad civil la persona jurídica “debe responder por los perjuicios resultantes de los actos cometidos por los subalternos, cualquiera que sea el vínculo jurídico que cree esta subordinación, siempre y cuando ellos actúen en ejercicio de las funciones encomendadas por la persona jurídica, o con motivo de las mismas”[86], pues se entiende que todo acto o hecho ejecutado, en ejercicio de sus funciones, por un subalterno se realiza para favorecer a la persona jurídica misma.

Exigir responsabilidad a las personas jurídicas por delitos relacionados con la ciberdelincuencia supone un avance en la garantía de derechos consagrados en la

Constitución y promueve la efectividad de los deberes y fines del Estado de que trata el artículo 2 superior. Asimismo, se cumple con los compromisos adquiridos por Colombia en el contexto internacional, en especial con la "Convención de las Naciones Unidas contra la delincuencia organizada trasnacional y el Protocolo para prevenir, reprimir y sancionar la trata de personas especialmente mujeres y niños que complementa la convención de las naciones unidas contra la delincuencia organizada trasnacional", adoptada por la Asamblea General de las Naciones Unidas el 15 de noviembre de 2000, declarada exequible en la Sentencia C-962 de 2003, así como la Ley 800 de marzo 13 de 2003 que la aprueba.

No obstante, toda norma o medida legislativa que resulte necesaria para que se pueda exigir responsabilidad a las personas jurídicas por los delitos previstos de conformidad con el presente Tratado, deberá respetar los límites constitucionales. De igual manera, la presente sentencia no puede tener efectos de cosa juzgada frente a los desarrollos normativos posteriores, los cuales estarán sujetos a los controles de constitucionalidad consagrados en la Constitución Política.

Finalmente, sobre las sanciones efectivas, proporcionadas y disuasorias de que trata el artículo 13 del Convenio, la Corte precisa que los fines de las penas y las sanciones derivadas de la implementación de estas medidas punitivas deberán armonizarse con los fines constitucionales de la pena, en los términos de valores y principios superiores; en especial del artículo 29 de la C. P.

3.2.3.1 Sección 2 (artículos 14 al 21) Derecho procesal

La sección 2 del instrumento comprende los siguientes títulos: 1. Disposiciones comunes (arts. 14 y 15); 2. Conservación rápida de datos informáticos almacenados (arts. 16 y 17); 3. Orden de prestación (art. 18); 4. Registro y confiscación de datos informáticos almacenados (art. 19); 5. Obtención en tiempo real de datos informáticos (arts. 20, 21 y 22).

En este capítulo se consagra la legislación procesal referente al Tratado, mediante la configuración de los procedimientos y poderes asignados a las autoridades públicas en cada uno de los Estados parte y con el fin de que adopten las directrices allí estipuladas a su derecho interno[87].

El Convenio sobre la Ciberdelincuencia impone las siguientes obligaciones:

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.

Título 1. Disposiciones comunes (arts. 14 y 15)

Los artículos 14 y 15 del Convenio consagran las reglas para la aplicación de las disposiciones contenidas en los artículos 16 al 21.

En este acápite se establece el ámbito de aplicación de las disposiciones comunes sobre los procedimientos con fines de investigación o procesos penales específicos y las condiciones y salvaguardas que aseguren su establecimiento, ejecución y aplicación con sujeción al derecho interno del Estado parte.

Las reglas comunes son las siguientes:

1. Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para establecer los poderes y procedimientos previstos en la Sección 2 para los fines de investigaciones o procedimientos penales específicos.

2. De igual manera, lo dispuesto en la Sección 2 se aplicará a los delitos previstos en los artículos 2 al 11 del presente Convenio, a otros delitos cometidos por medio de un sistema informático y a la obtención de pruebas electrónicas de un delito.

El numeral 3 del artículo 14 regula la posibilidad de reserva. Señala que cualquier parte podrá reservarse el derecho a aplicar las medidas indicadas en el artículo 20[88]

exclusivamente a los delitos especificados en la reserva procurando siempre la aplicación más amplia posible del objeto del Tratado.

De igual manera, se establece que como consecuencia de las limitaciones existentes en la legislación interna, las Partes podrán no 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 comunicación ni esté conectado a otro sistema informático, ya sea público o privado.

El artículo 15 consagra las condiciones y salvaguardas para aplicación de los artículos 16 y 21 y que son de la mayor importancia en el análisis de constitucionalidad del presente Tratado:

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. (Subrayado fuera del texto)

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.

Análisis de constitucionalidad de la Sección 2

A efectos de realizar el control de constitucionalidad, resulta importante resaltar las condiciones y salvaguardas necesarias para la aplicación de los artículos 16 al 21. En primer lugar, las medidas adoptadas (i) están sujetas a las condiciones y salvaguardas previstas en su derecho interno, las cuales deben garantizar el respeto pleno de las garantías fundamentales, (ii) en el caso que el derecho interno lo disponga, resultará necesaria la intervención judicial y (iii) deben protegerse los derechos de los terceros.

Lo anterior garantiza entonces que la aplicación de todas las medidas dispuestas en el Tratado, especialmente las consagradas en la Sección 2, están sometidas a la normatividad colombiana, así como a las limitaciones dispuestas en la Constitución Política.

Por otro lado, de conformidad con los antecedentes del Proyecto de Ley número 58 de 2017 Senado, el Ejecutivo indicó que "formulará una reserva al artículo del tratado, con miras a proteger los derechos constitucionales del habeas data y la intimidad personal". Aunado a lo anterior, se informó que "también se plantea la posibilidad de reservar la aplicación del artículo 21, concerniente a la "Interceptación de datos relativos al contenido"[89], en los casos en que un sistema informático: i) se haya puesto en funcionamiento para un grupo restringido de usuarios y ii) no emplee las redes públicas de telecomunicaciones y no esté conectado a otro sistema informático, ya sea público o privado.

Asimismo, durante el trámite del control de constitucionalidad de la Ley 1928 de 2018, "Por medio de la cual se aprueba el convenio sobre la ciberdelincuencia", en cumplimiento de lo requerido en Auto 064 de 2019[90], la Directora de Asuntos Jurídicos Internacionales del Ministerio de Relaciones Exteriores se pronunció sobre el alcance de la referida reserva indicando el sentido de la misma en los siguientes términos: "de conformidad con el artículo 14, párrafo 3, y frente a los artículos 20 y 21 del Convenio, Colombia se reserva el derecho de aplicar las medidas referidas en los mencionados artículos de conformidad con su normativa interna en materia de habeas data y protección del derecho a la intimidad".

Finalmente, se tiene que durante el trámite legislativo del Proyecto de Ley 058 de 2017 Senado "Por medio de la cual se aprueba el Convenio sobre la Ciberdelincuencia", adoptado el 25 de noviembre de 2001 en Budapest, el Consejo Superior de Política Criminal profirió el Concepto 06.2018, el 4 de septiembre de 2017, con el fin de respaldar la reserva formulada por la rama ejecutiva. En la referida valoración técnica se afirma que:

“Este órgano colegiado resulta ser conveniente, pues la aplicación de estas disposiciones puede entrar en contradicción con los derechos y las garantías fundamentales contempladas en la Constitución Política.

Los citados artículos propenden por la obtención de datos, en tiempo real, lo cual puede implicar una afectación al derecho la intimidad personal, el cual en los términos de la Corte Constitucional es de carácter fundamental e inalienable, siendo el titular de este, el único legitimado para permitir la divulgación de datos relativos a su vida privada[91]. En adición a ello, el artículo 15º superior estableció que todas las formas de comunicación son de carácter privado, salvo en los casos de registro o la interceptación por orden judicial, con el debido cumplimiento de las formalidades establecidas por la ley, razón por la cual la adhesión integral al Convenio implicaría la flagrante vulneración del ordenamiento jurídico interno en relación con el derecho a la intimidad”. (Negrilla agregada).

De lo anterior se concluye que (i) el mismo Tratado dispone que las disposiciones del convenio se aplicarán de conformidad con el derecho interno, (ii) en aras de garantizar la vigencia del ordenamiento constitucional el Gobierno se reservará el derecho de aplicar las medidas referidas en los artículos 20 y 21 de conformidad con la normativa interna en materia de habeas data y protección a la intimidad. Cabe señalar que los artículos 20 y 21 se refieren a la interceptación del contenido en tiempo real, a diferencia de los artículos 16, 17, 18 y 19 que estipulan las medidas legislativas y de otro tipo para la conservación rápida de datos informáticos almacenados.

Encuentra la Sala Plena procedente la reserva planteada por parte del Estado colombiano, la cual deberá formularse en los estrictos términos de la Constitución Política de 1991, como una manifestación de voluntad que surtirá efectos jurídicos a partir del momento en que Colombia notifique por escrito al Secretario General del Consejo de Europa su intención de depositar el instrumento de adhesión al Convenio sobre la Ciberdelincuencia, frente a la aplicación de los artículos 20 y 21 de dicho instrumento internacional, por las razones que se exponen a continuación:

Protección del derecho a la intimidad

El artículo 15 de la Constitución Política reconoce el derecho a la intimidad personal y familiar, y establece expresamente el derecho de todas las personas a su buen nombre y el

deber del Estado de respetar y hacer respetar esos derechos.

La Corte Constitucional ha sostenido que el objeto del derecho a la intimidad es "garantizar a las personas una esfera de privacidad en su vida personal y familiar, al margen de las intervenciones arbitrarias que provengan del Estado o de terceros" y que "la protección frente a la divulgación no autorizada de los asuntos que conciernen a ese ámbito de privacidad" forma parte de esta garantía[92].

De igual manera, esta Corporación en la Sentencia C-640 de 2010 señaló que el derecho a la intimidad "permite a las personas manejar su propia existencia como a bien lo tengan con el mínimo de injerencias exteriores" y que la protección "de esa esfera inmune a la injerencia de los otros –del Estado o de otros particulares" es un "prerrequisito para la construcción de la autonomía individual que a su vez constituye el rasgo esencial del sujeto democráticamente activo".[93]

En ese orden de ideas, el área restringida que constituye la intimidad "solamente puede ser penetrada por extraños con el consentimiento de su titular o mediando orden dictada por autoridad competente, en ejercicio de sus funciones y de conformidad con la Constitución y la ley"[94]. Lo anterior, en desarrollo a los cinco principios que garantizan la protección de la esfera privada frente a injerencias externas injustificadas, a saber:

"(i) Libertad, hace referencia a que sin existir obligación impuesta por parte del ordenamiento jurídico o sin contar con el consentimiento o autorización del afectado, los datos de una persona no pueden ser divulgados, ni registrados, pues de lo contrario, se constituye una conducta ilícita;

(ii) Finalidad, en virtud del cual la publicación o divulgación de los datos personales solo puede ser permitida si con ello se persigue un interés protegido constitucionalmente como el interés general en acceder a determinada información;

(iii) Necesidad, implica que los datos o información que se va a revelar guarden relación con un soporte constitucional;

(iv) Veracidad, por lo que se encuentra prohibida la publicación de información personal que no se ajuste a la realidad o sea incorrecta; y,

(v) Integridad, que indica que no puede evidenciarse parcialidad o fragmentación en los datos que se suministran, es decir, que la información debe ser completa"[95].

La sujeción a estos principios permite una legítima divulgación de la información personal al igual que garantizar que el proceso de publicación y comunicación sea el adecuado[96].

El derecho a la intimidad está protegido por múltiples garantías constitucionales e instrumentos de orden internacional. En especial, el artículo 12 de la Declaración Universal de los Derechos Humanos dispone: "Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques".

En igual sentido, el artículo 17.1 del Pacto Internacional de Derechos Civiles y Políticos, ratificado por el Congreso de la República mediante la Ley 74 de 1968 dispone que: "Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. Toda persona tiene derecho a la protección de ley contra esas injerencias o esos ataques", prohibición reiterada en el artículo 11.2 de la Convención Americana sobre Derechos Humanos, ratificada por Colombia mediante la Ley 16 de 1972 que prescribe: "Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques."

Sobre la interceptación de comunicaciones en el ordenamiento jurídico interno

Dentro del marco normativo colombiano, en materia procesal penal la Ley 600 de 2000 "Por la cual se expide el Código de Procedimiento Penal" fijó una limitación funcional a la interceptación a las comunicaciones, determinando que este procedimiento investigativo comporta una facultad exclusiva de los funcionarios judiciales. Así, el artículo 301 de la referida norma establece:

"Interceptación de comunicaciones. El funcionario judicial podrá ordenar, con el único objeto de buscar pruebas judiciales, que se intercepten mediante grabación magnetofónica las comunicaciones telefónicas, radiotelefónicas y similares que utilicen el espectro

electromagnético, que se hagan o reciban y que se agreguen al expediente las grabaciones que tengan interés para los fines del proceso. En este sentido, las entidades encargadas de la operación técnica de la respectiva interceptación, tienen la obligación de realizar la misma dentro de las cuarenta y ocho (48) horas siguientes a la notificación de la orden.

A su turno, el artículo 316 de citado marco legal, estableció una restricción expresa a la policía judicial para la práctica de interceptación a las comunicaciones. El tenor de la norma en cita es el siguiente:

"Artículo 316. Actuación durante la investigación y el juzgamiento. Iniciada la investigación la policía judicial sólo actuará por orden del fiscal, quien podrá comisionar a cualquier servidor público que ejerza funciones de policía judicial para la práctica de pruebas técnicas o diligencias tendientes al esclarecimiento de los hechos, lo cual podrá ser ordenado y comunicado por cualquier medio idóneo, dejando constancia de ello. La facultad de dictar providencias interlocutorias es indelegable.

Los miembros de policía judicial pueden extender su actuación a la práctica de otras pruebas técnicas o diligencias que surjan del cumplimiento de la comisión, excepto capturas, allanamientos, interceptación de comunicaciones, las que atenten contra el derecho a la intimidad o cualquier actividad que represente la vinculación de los implicados a la actuación procesal.

Por comisión del juez respectivo, en la etapa del juzgamiento cumplirán las funciones en la forma indicada en los incisos anteriores." (Negrillas fuera del texto).

La Ley 906 de 2004, "Por la cual se expide el Código de Procedimiento Penal", modificada por el artículo 15[97] de la Ley 1142 de 2007[98] y por el artículo 52[99] de la Ley 1453 de 2011[100], reguló de manera integral el procedimiento de las interceptaciones de comunicaciones.

Así, prevé cuatro disposiciones relativas a la interceptación a las comunicaciones, a saber: (i) el artículo 14[101] establece como principio rector de la actuación procesal el derecho a la intimidad; (ii) el artículo 154.1[102] regula las distintas modalidades de audiencia preliminar y ordena "…poner a disposición del juez de control de garantías los elementos recogidos en registros, allanamientos e interceptación de comunicaciones ordenadas por la

Fiscalía, para su control de legalidad dentro de las treinta y seis (36) horas siguientes"; (iii) el artículo 235 versa sobre la finalidad de la interceptación a las comunicaciones y, finalmente, (iv) el artículo 237[103] regula la audiencia de control de legalidad posterior, la cual está a cargo del juez de control de garantías.

Sobre la finalidad de la interceptación a las comunicaciones, el artículo 235[104] de la citada Ley 906 de 2004 dispone:

"Artículo 235. Interceptación de comunicaciones. El fiscal podrá ordenar, con el objeto de buscar elementos materiales probatorios, evidencia física, búsqueda y ubicación de imputados, indiciados o condenados, que se intercepten mediante grabación magnetofónica o similares las comunicaciones que se cursen por cualquier red de comunicaciones, en donde curse información o haya interés para los fines de la actuación. En este sentido, las autoridades competentes serán las encargadas de la operación técnica de la respectiva interceptación así como del procesamiento de la misma. Tienen la obligación de realizarla inmediatamente después de la notificación de la orden y todos los costos serán a cargo de la autoridad que ejecute la interceptación" (negrillas fuera de texto).

El artículo 237 de la Ley 906 de 2004[105] establece una audiencia de control de garantías, posterior a la realización de la interceptación a las comunicaciones. La norma en cita dispone:

"Artículo 237. Audiencia de control de legalidad posterior. Dentro de las veinticuatro (24) horas siguientes al diligenciamiento de las órdenes de registro y allanamiento, retención de correspondencia, interceptación de comunicaciones o recuperación de información dejada al navegar por internet u otros medios similares, el fiscal comparecerá ante el juez de control de garantías, para que realice la audiencia de revisión de legalidad sobre lo actuado".

El artículo 81 de la Ley 1453 de 2011[106] otorga al Fiscal la facultad de decretar la práctica de interceptaciones como técnica de investigación y debe ser ordenada en la fase inicial de la investigación.

De otro lado, el artículo 1 del Decreto 1704 de 2012 "por medio del cual se reglamenta el artículo 52 de la Ley 1453 de 2011, se deroga el Decreto 075 de 2006 y se dictan otras

disposiciones", definió la interceptación legal de comunicaciones como "un mecanismo de seguridad pública que busca optimizar la labor de investigación de los delitos que adelantan las autoridades y organismos competentes, en el marco de la Constitución y la ley", cualquiera que sea el origen o tecnología utilizada.

Finalmente, la Ley Estatutaria 1621[107] de 2013[108] regula la interceptación a las comunicaciones como herramienta investigativa y dispone que sólo puede efectuarse en el marco de los procesos judiciales y, con observancia del artículo 15 de la Constitución Política.

Del anterior recuento normativo se observa que el ordenamiento jurídico colombiano exige la intervención judicial a efectos de ordenar la interceptación de comunicaciones ya sea directamente o a través de la intervención posterior del juez de control de garantías. Esta ha sido además la regla reiterada constantemente por el Tribunal Constitucional, como se expone a continuación.

Sobre la interceptación de comunicaciones en la jurisprudencia constitucional

En materia de interceptación a las comunicaciones, la Corte Constitucional en Sentencia C-626 de 1996[109] indicó que las que las intromisiones en las comunicaciones de los particulares, sólo pueden adelantarse previa orden de la autoridad judicial competente y con el cumplimiento de las formalidades establecidas en la ley. En esa oportunidad manifestó: "(…) ninguna persona pública ni privada, por plausible o encomiable que sea el objetivo perseguido, está autorizada para interceptar, escuchar, grabar, difundir ni transcribir las comunicaciones privadas, esto es, las que tienen lugar entre las personas mediante conversación directa, o por la transmisión o registro de mensajes, merced a la utilización de medios técnicos o electrónicos aptos para ello, tales como teléfonos convencionales o celulares, radioteléfonos, citófonos, buscapersonas, equipos de radiocomunicaciones, entre otros, A MENOS QUE EXISTA PREVIA Y ESPECIFICA ORDEN JUDICIAL Y QUE ELLA SE HAYA IMPARTIDO EN EL CURSO DE PROCESOS, EN LOS CASOS Y CON LAS FORMALIDADES QUE ESTABLEZCA LA LEY, según los perentorios términos del artículo 15 de la Constitución Política" (negrilla agregada).

El carácter de inviolabilidad de las comunicaciones privadas y la necesidad de orden judicial fue reiterado en la Sentencia C-692 de 2003, mediante la cual se juzgó la

constitucionalidad de varias disposiciones de la Ley 746 de 2002[110]. Para la Corte, "la Constitución prevé que la correspondencia y demás formas de comunicación privada son inviolables y que las mismas sólo pueden ser interceptadas o registradas mediante orden judicial en los casos y con las formalidades que la ley determine (negrilla agregada).

En la Sentencia C-336 de 2007, mediante la cual esta Corporación se pronunció en torno al control posterior ejercido por el juez de control de garantías, la Sala Plena enfatizó en la exigencia constitucional de contar con orden judicial previa para la interceptación a las comunicaciones:

"El acopio de información en relación con las personas puede ser eventualmente un medio necesario para la satisfacción de ese interés constitucionalmente protegido. Sin embargo, su recaudo debe realizarse con escrupuloso acatamiento de las cautelas que la propia Constitución ha establecido para la protección de los derechos fundamentales especialmente expuestos a su afectación, vulneración o mengua en el contexto de una investigación criminal. El requerimiento de autorización judicial previa para la adopción de medidas –adicionales- que implique afectación de derechos fundamentales es una de esas cautelas que el legislador debe acatar al configurar las reglas orientadas a regular la actividad investigativa del Estado".

En esa providencia la Corte se refirió al control posterior a cargo del juez de control de garantías en los siguientes términos:

"Para determinar el tipo de control que debe recaer sobre las medidas a que se refieren las normas demandadas, conviene recordar las reglas que deslindan la actuación de la Fiscalía y del juez de control de garantías en materia de facultades de afectación de derechos fundamentales, conforme al artículo 250 superior: (i) corresponde a los jueces de control de garantías la adopción de las medidas necesarias para asegurar la comparecencia de los imputados al proceso penal; solo excepcionalmente y previa regulación legal que incluya los límites y eventos en que procede, la Fiscalía puede efectuar capturas; (ii) la Fiscalía tiene la facultad de adelantar registros, allanamientos, incautaciones e interceptación de comunicaciones, sometidos al control posterior del juez de control de garantías; y (iii) en todos los demás eventos en que para el aseguramiento de los elementos materiales probatorios, se requiera medidas adicionales que impliquen afectación de derechos

fundamentales, deberá mediar autorización, es decir, control previo, por parte del juez de control de garantías." (Negrilla agregada).

En cuanto al control posterior a las interceptaciones, la Corte por medio de la Sentencia C-025 de 2009[111] se pronunció con respecto al fundamento jurídico de la audiencia de control de garantías durante la fase investigativa del proceso penal, en los siguientes términos:

"La audiencia de control o revisión de legalidad posterior que se cumple por parte del Juez de Control de Garantías sobre la práctica de ciertas diligencias realizadas, bien durante la indagación previa o bien durante la etapa de investigación, por parte de la Fiscalía General de la Nación y los órganos de Policía Judicial sin previa autorización judicial para su realización, comprende las medidas de: (i) registro y allanamiento, retención de correspondencia, interceptación de comunicaciones o recuperación de información dejada al navegar por internet u otros medios similares; (ii) actuación de agentes encubiertos; (iii) entrega vigilada de objetos; (iv) búsqueda selectiva en base de datos y (v) práctica de exámenes de ADN, y tiene como propósito específico llevar a cabo la revisión formal y sustancial del procedimiento utilizado en la práctica de las citadas diligencias, esto es, verificar que se hayan respetado los parámetros constitucionales y legales establecidos para su autorización y realización, e igualmente, que la medida de intervención no haya desconocido garantías fundamentales".

Estas mismas reglas fueron reiteradas en las Sentencias C-594 de 2014[112] y SU- 414 de 2017[113].

Protección del derecho al habeas data

Por otra parte, el Gobierno colombiano también realizará reserva encaminada a la protección del derecho al habeas data. Por lo anterior, la Sala procederá a efectuar una breve reseña legal y jurisprudencial del mismo.

El derecho fundamental al habeas data se encuentra regulado en la Ley 1581 de 2012[114], se define como una garantía constitucional que "permite a las personas naturales y jurídicas conocer, actualizar y rectificar la información que sobre ellas se haya recogido en bancos de datos y en archivos de entidades públicas y privadas"[115]. Este

derecho “implica deberes de conservación documental a cargo de las entidades que custodian y administran la información contenida en archivos y bases de datos, necesaria para acceder al goce efectivo de otros derechos fundamentales”[116].

La Sala Quinta de Revisión de la Corte Constitucional en la Sentencia T-207A de 2018 reiteró los principios que deben prevalecer en el tratamiento de datos personales como una garantía del derecho fundamental al habeas data. A saber: “(i) principio de libertad; (ii) principio de necesidad; (iv) principio de integridad; (v) principio de finalidad; (vi) principio de utilidad; (vii) principio de incorporación; y, (viii) principio de caducidad.

Para la Corte estos principios implican deberes constitucionales para las entidades que custodian, conservan y administran la información contenida en bases de datos. Así, recae en cabeza de dichas entidades la obligación general de brindar seguridad y diligencia en la administración y conservación de los datos personales y evitar el mal manejo de la información[117].

En este orden de ideas, se observa que las medidas de la Sección 2 que a continuación se refieren deben ser aplicadas: (i) de conformidad con las limitaciones, restricciones y procedimientos establecidos en el orden interno, previamente descrito (tal y como lo dispone en mismo texto del tratado) y (ii) en aras de garantizar la vigencia del ordenamiento constitucional, especialmente en relación con la aplicación de los artículos 20 y 21 del Tratado, el Gobierno se reservará el derecho de aplicar las medidas referidas de conformidad con la normativa interna en materia de habeas data y protección a la intimidad.

De otro lado, el artículo 15 sobre las condiciones y salvaguardas del Título 1 del Capítulo II – Sección 2, constituye una herramienta interpretativa importante para el análisis del Tratado, en la medida en que sus disposiciones condicionan al Estado Parte a asegurar que el establecimiento, la ejecución y la aplicación de los poderes y procedimientos previstos en la referida Sección estén sujetos al principio de proporcionalidad y a las condiciones, libertades y salvaguardas previstas en su derecho interno.

Asimismo, insiste en que la administración de justicia en cumplimiento del Tratado se ejecute con la estricta observancia de los derechos derivados de las obligaciones asumidas, entre otros, en el Pacto Internacional de derecho civiles y políticos de la Naciones Unidas y

de otros instrumentos internacionales aplicables en materia de derechos humanos. En este contexto, los artículos comprendidos en el Título 2 de la Sección 2, guardan consonancia con las disposiciones constitucionales.

Sobre la reserva anteriormente analizada la Universidad Sergio Arboleda sugirió a la Corte Constitucional que la misma se aplicara a delitos graves; específicamente, la universidad se refirió a todos los tipos penales contemplados en los títulos I, III, IV, VII, VII Bis, VIII y XII del libro segundo del Código Penal.

No obstante, considera la Sala Plena de esta Corporación que en razón a que toda la normativa se encuentra sometida al derecho interno y por ende a todas las garantías del mismo, no es necesario ampliar la formulación de la reserva frente a todos los delitos referidos por la interviniente, pues el ordenamiento interno cuenta con los mecanismos y procedimientos necesarios para la protección de los derechos constitucionales en juego y la adhesión de Colombia al Convenio suministrará las herramientas necesarias para desarrollar acciones coordinadas de forma ágil frente a conductas de ciberdelincuencia que atenten contra los mismos.

Establecida la procedencia de la reserva que realizará el Ejecutivo, la cual, se reitera, deberá respetar los términos de la Constitución Política, en relación con el artículo 14 del Tratado, se procederá a analizar si las restantes disposiciones de la Sección Segunda se encuentran acordes con el ordenamiento superior.

Análisis de constitucionalidad de los artículos 16 al 21 del Convenio sobre la Ciberdelincuencia

Para comprender la estructura de esta sección segunda cabe señalar que se divide en tres grandes asuntos. Así: (i) los artículos 16 y 17 se refieren a la conservación rápida de datos informáticos almacenados y de datos sobre el tráfico; (ii) los artículos 18 y 19 preceptúan lo correspondiente a la presentación, la confiscación y el registro de datos informáticos almacenados en un sistema informático; y (iii) los artículos 20 y 21 establecen la posibilidad de interceptación de datos sobre el contenido de determinadas comunicaciones en el territorio del Estado parte, transmitida por medio de un sistema informático.

La Sala observa que los tres grupos de preceptos que conforman la Sección 2 del Convenio

se encuentran sometidos al derecho interno. Se resalta que ante el impacto a los derechos a la intimidad y al habeas data, en relación con la posible interceptación en tiempo real de datos sobre el contenido (artículos 20 y 21), el Estado colombiano realizará la correspondiente reserva.

La Sección 2 del Convenio, luego de establecer las reglas de aplicación comunes, se divide en varios títulos, a saber:

El título 2 de la Sección 2 del Convenio, Conservación rápida de datos informáticos almacenados (arts. 16 y 17), se refiere a las medidas legislativas y de otro tipo que resulten necesarias para permitir a las autoridades competentes de la Parte ordenar o imponer la conservación rápida de datos informáticos y de datos sobre el tráfico; así como su revelación, custodia y evitar su pérdida o modificación. Lo anterior, aplicable a lo dispuesto en los artículos 14 y 15 del Tratado.

El literal b del artículo 1 del Tratado de la referencia define 'datos informáticos' como "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". Asimismo, el literal d de la norma citada precisa que 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".

Los artículos 16 y 17 del Convenio sobre la Ciberdelincuencia hacen referencia únicamente al almacenamiento de datos informáticos y de datos sobre el tráfico; en esa medida, se debe entender que no se refieren a la divulgación del contenido de los mismos, pues, como el Tratado lo específica, se trata exclusivamente de garantizar su conservación, circunstancia que no riñe con ninguna de las garantías constitucionales del Estado colombiano.

El Título 3 regula en su artículo 18 que cada parte podrá, mediante medidas legislativas o de otro tipo previamente establecidas, facultar a las autoridades competentes para ordenar a una persona que se encuentre en su territorio el suministro de 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.

A efectos del presente Convenio se entenderá por 'sistema informático' "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" (art. 1, literal a, Convenio de Budapest).

Las autoridades competentes podrán ordenar 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.

El literal c del artículo 1 del Convenio sobre la Ciberdelincuencia indica que por 'proveedor de servicios' se entenderán:

"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".

El Título 4 regula el "Registro y confiscación de datos informáticos almacenados" (art. 19). El Tratado dispone que las autoridades competentes de cada Estado parte puedan registrar o tener acceso a los datos almacenados en sistemas informáticos o a una parte del mismo y que se encuentren en su territorio.

Cabe de igual manera señalar que el artículo 19 del Convenio alude a la facultad de confiscación de datos informáticos almacenados. Esta debe entenderse en el ordenamiento interno equiparada a la medida del comiso o decomiso penal de que trata el artículo 100 del Código Penal de nuestro ordenamiento[118]. En ningún caso, el registro, confiscación o incautación de los datos informáticos almacenados dará lugar a la relevación o exposición de su contenido, entendiéndose que se trata de información confidencial.

Finalmente, el Título 5 del Capítulo II, Obtención en tiempo real de datos informáticos, dispone que cada Parte adoptará las medidas legislativas y de otro tipo que faculten a sus autoridades competentes para la obtención en tiempo real de datos sobre el tráfico e interceptación de datos sobre el contenido, asociados a comunicaciones especificas en su

territorio por medio de un sistema informático.

Las medidas legislativas y de otro tipo de que tratan los artículos 20 y 21 del Convenio sobre la Ciberdelincuencia, a diferencia de los artículos 16, 17, 18 y 19, sí se refieren específicamente al contenido de la información obtenida y a su posible divulgación para verificar o comprobar la configuración de delitos graves cometidos en el Estado Parte. En esa medida, el Gobierno colombiano anunció la correspondiente reserva analizada previamente en el numeral 3.2.3.1, Sección 2, Título 1, de la presente sentencia. Lo anterior, con el fin de que el acceso al contenido mismo de la información privada sea realizado con total apego al ordenamiento constitucional en materia de garantía de los derechos fundamentales a la intimidad y al habeas data, como se determinó al abordar el estudio de constitucionalidad de los artículos 14 y 15 del Convenio sobre la Ciberdelincuencia.

3.2.3.2. Análisis de constitucionalidad de la Sección 3. Jurisdicción (art. 22)

En la Sección 3, del Capítulo II se incluye el tema relativo a la Jurisdicción (art. 22), indica el Convenio que cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para afirmar su jurisdicción en cualquier delito previsto en el presente Tratado y cometido en su territorio, en un buque que enarbole el pabellón de dicho país o por uno de sus nacionales.

De lo expuesto la Sala Plena Concluye que el Capítulo II del Convenio sobre la Ciberdelincuencia objeto de examen, se adecua y respeta las reglas y principios constitucionales, y guarda armonía con los artículos 2, 9, 15, 20, 29, 34, 44, 58, 61, 113, 116, 226, 226, 227, 228, 229, 230 y 250 de la C. P.

3.2.4. Constitucionalidad de las normas contenidas en el Capítulo III. Cooperación internacional (artículos 23 al 35)

3.2.4.1. Sección 1. Principios generales

La sección 1 de este capítulo comprende los siguientes títulos: 1. Principios generales relativos a la cooperación internacional (art. 23); 2. Principios relativos a la extradición (art. 24); 3. Principios generales relativos a la asistencia mutua (arts. 25 y 26); 4.

Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables (arts. 27 y 28);

Esta primera parte del Capítulo III establece como eje del Convenio la cooperación internacional, se fijan en este apartado los principios generales (sección 1, título 1) de los mecanismos allí incluidos, así como los principios relativos a la extradición (sección 1, título 2) y los procedimientos con relación a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables.

Así, se describen una a una las pautas mínimas de colaboración internacional entre Estados en materia penal que contribuyan a las investigaciones y procedimientos relativos a los delitos relacionados con sistemas y datos informáticos (art. 23). Lo anterior, en términos de equidad, reciprocidad y conveniencia nacional.

Sobre el artículo referido a la extradición, resulta necesario indicar que se debe entender en armonía con los motivos de denegación dispuestos en los artículos 25.4 y 27.4 del Convenio. A saber:

Artículo 25, numeral 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 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".

(…)

Artículo 27, numeral 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".

Encuentra la Sala que la disposición anteriormente descrita debe entenderse como una cláusula interpretativa que reafirma el principio de soberanía contenido en el artículo 9 de la Constitución Política como rector de las relaciones internacionales. En ese contexto, el Convenio sobre la Ciberdelincuencia en materia de extradición autoriza a una Parte a rehusarse a prestar asistencia cuando la ejecución de la solicitud atente contra su soberanía, seguridad, orden público u otros intereses esenciales.

Lo anterior, en concordancia con los elementos decantados por esta Corporación sobre el principio de soberanía nacional: "(i) el entendimiento de la soberanía como independencia, en especial frente a Estados con pretensiones hegemónicas; (ii) la aceptación de que adquirir obligaciones internacionales no compromete la soberanía, así como el reconocimiento de que no se puede invocar la soberanía para retractarse de obligaciones válidamente adquiridas; y (iii) la reafirmación del principio de inmediación según el cual el ejercicio de la soberanía del Estado está sometido, sin intermediación del poder de otro Estado, al derecho internacional"[119].

3.2.4.2. Sección 2. Disposiciones especiales

La Sección 2 del Capítulo III contiene los Título: 1. Asistencia mutua en materia de medidas provisionales (arts. 29 y 30); 2. Asistencia mutua en relación con los poderes de investigación (arts. 31, 32, 33 y 34); y, 3. Red 24/7 (art. 35).

Las disposiciones contenidas en esta sección se encaminan a facilitar la cooperación efectiva entre las Partes, mediante compromisos relacionados con la asistencia mutua en materia de medidas provisionales, asistencia mutua respecto a los poderes de investigación y designación de puntos de contacto que constituirán una red con disponibilidad permanente.

Sobre el artículo 29 del Convenio sobre la Ciberdelincuencia, "Conservación rápida de datos informáticos almacenados", la Universidad Sergio Arboleda sugirió a esta Corporación la posibilidad de exigir la aplicación de la cláusula de reserva del numeral 4 del referido precepto[120]. Al respecto, la Corte reitera que el establecimiento, la ejecución y la

aplicación de los procedimientos previstos en el presente Tratado están sujetos a las condiciones y salvaguardas previstas en el derecho interno de Colombia. En ningún caso, las disposiciones de carácter general o especial del Convenio podrán efectuarse en contra del marco legal o de la Constitución Política; en esa medida, la propuesta planteada por la universidad interviniente no tiene vocación de procedencia.

Entre otros temas, se regula la obtención de pruebas en formato electrónico, el intercambio rápido y efectivo de algunos casos confidenciales, el acceso transfronterizo en la obtención, confiscación, aseguramiento y conversación de datos que se encuentran en el territorio de otra Parte a solicitud del país signatario interesado y la designación de puntos de contacto que constituirán una red con disponibilidad permanente – Red 24/ (art. 35).

Para la Sala estas disposiciones son constitucionales, por cuanto se encaminan a facilitar la cooperación efectiva entre las Partes y proporcionan mecanismos que aseguran la implementación y promoción del Convenio, las cuales de manera general resultan compatibles con la Constitución y promueven la efectividad de los compromisos contraídos por los países signatarios, que busca la consecución pacifica de los objetivos del instrumento internacional, lo cual se halla en armonía con los principios del derecho internacional aceptados por Colombia.

Bajo estas consideraciones, se concluye que el Capítulo III del Convenio sobre la Ciberdelincuencia atiende las reglas y principios constitucionales, en especial lo preceptuado en los artículos 2, 9, 29, 35, 226 y 227 de la Constitución Política de 1991.

Por último, los artículos 36 al 48 del Convenio sobre la Ciberdelincuencia regulan aspectos procedimentales propios de cualquier tratado internacional que de ninguna manera vulneran la Constitución Política.

En este capítulo se introducen ciertas formas propias de los acuerdos internacionales, asociadas a la firma y entrada en vigor del Convenio, la posibilidad de adhesión de Estados que no sean miembros del Consejo de Europa, la aplicación territorial, los efectos del instrumento, las declaraciones mediante notificaciones sobre elementos complementarios, la “cláusula federal” (que permite a los Estados federales a reservarse el derecho de asumir las obligaciones derivadas del capítulo II del Convenio), las reservas y retiro de las mismas, enmiendas, soluciones de controversias, consultas entre partes, denuncia y

notificaciones.

En este orden, se establece que el presente Convenio estará abierto a la firma y sujeto a la ratificación, aceptación o aprobación de los Estados miembros del Consejo de Europa y de los Estados no miembros que hayan participado en su elaboración. Respecto de cualquier Estado signatario que exprese 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 que haya expresado su voluntad de vincularse, de conformidad con lo dispuesto en el aparte 1 del artículo 36.

Para todo Estado que se adhiera al Convenio, éste 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 (art. 37). El Estado podrá especificar el territorio o territorios a los que se aplicará el Convenio (art. 38).

El Convenio sobre la Ciberdelincuencia tiene como finalidad completar los tratados o acuerdos multilaterales o bilaterales aplicables entre las Partes, entre otros, el Convenio europeo de asistencia judicial en materia penal, abierto a firma en Estrasburgo el 20 de abril de 1959, y el Protocolo adicional al Convenio europeo de asistencia judicial en materia penal, abierto a firma en Estrasburgo el 17 de marzo de 1978, (art. 39).

Los Tratados de la Unión Europea son acuerdos vinculantes entre los países miembros. Establecen los objetivos de la UE, las normas de las instituciones europeas, la manera en que se toman las decisiones y la relación entre la Unión y sus miembros.

En ese contexto, se precisa que la adhesión de Colombia al Convenio sobre la Ciberdelincuencia no implica la aprobación por parte del Estado colombiano de los acuerdos internacionales a los que se refiere, por cuanto Colombia no los ha ratificado a través del trámite de constitucionalidad dispuesto para los tratados.

Cada Estado podrá, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión y mediante notificación por escrito dirigida al Secretario General del Consejo de Europa, declarar 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.,

(art. 40)[121].

Los Estados federales mediante cláusula podrán reservarse el derecho a asumir las obligaciones derivadas del Capítulo II del Convenio de forma compatible con los principios fundamentales que rijan la relación entre su gobierno central y los estados que lo formen (art. 41).

Al momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, cualquier Estado Parte podrá acogerse a una o varias de las reservas previstas en el presente Convenio, mediante notificación por escrito dirigida al Secretario General del Consejo de Europa. No podrán formularse otras reservas (art. 42). En ese contexto, la reserva que formulará el Gobierno Nacional en defensa de los derechos fundamentales a la intimidad y al habeas data surtirá efectos jurídicos a partir del momento en que el Estado colombiano notifique al Secretario General del Consejo de Europa sobre la adhesión al Convenio sobre la Ciberdelincuencia y anuncie que se acoge a la reserva contemplada en el artículo 14, numeral 3 del referido Tratado.

La reversa formulada podrá ser retirada en todo o en parte y surtirá efecto desde el momento en que el Secretario General reciba la notificación o desde la fecha que indique la Parte interesada (art. 43).

Cualquier Estado parte podrá proponer enmiendas al Convenio Sobre la Ciberdelincuencia y éstas serán comunicadas a todos los miembros de conformidad al artículo 37 del presente instrumento (art. 44).

Hay remisiones en cuanto al arreglo de controversias sobre la interpretación o aplicación del presente Convenio, las cuales se deberán resolver mediante negociaciones o por cualquier otro medio pacífico que las partes interesadas elijan (art. 45).

Las Partes se consultarán periódicamente con el objeto de facilitar la utilización y la aplicación de las medidas adoptadas en el Convenio, incluida la detección de cualquier problema derivado del mismo, así como los efectos de cualquier declaración o reserva formulada (art. 46).

Las Partes podrá denunciar el presente Convenio en cualquier momento, dicha acusación

surtirá efecto el primer día del mes siguiente a la expedición de un plazo de tres meses desde la fecha en que el Secretario General haya recibido la notificación (artículo 47).

Finamente, recae sobre el Secretario General del Consejo de Europa la obligación de notificar sobre cualquier acto relativo al presente Convenio (firma, depósito de ratificación, aceptación, aprobación o adhesión, entrada en virgo, declaración o reserva) a los Estados miembros de ese órgano, a los Estados no miembros que hayan participado en la elaboración del Convenio sobre la Ciberdelincuencia y a cualquier Estado que se haya adherido al mismo o que haya sido invitado a hacerlo (art. 48).

Encuentra la Corte que las disposiciones que regulan las clausulas relativas a la firma, la ratificación, la entrada en vigor, el depositario, la posibilidad de hacer reservas, así como aquellas que tratan sobre la aprobación de enmiendas, entre otras, reflejan aspectos operativos y técnicos propios de cualquier instrumento internacional multilateral que de ninguna manera vulneran la Constitución Política.

3.2.6. Conclusión

El Convenio sobre la Ciberdelincuencia se presenta como un instrumento internacional cuyo objetivo es intensificar la cooperación entre los Estados Parte del mismo, mediante la materialización de una política criminal común en contra de la comisión de delitos cibernéticos. Lo anterior, como una respuesta a los profundos cambios provocados por la digitalización, convergencia y globalización de datos y sistemas informáticos. De esta manera, al establecer las condiciones para prevenir la comisión de ilícitos en las redes informáticas, compromete a los países signatarios a adoptar su legislación interna para combatir posibles amenazas a bienes jurídicos tutelados como la confidencialidad, la integridad y la disponibilidad de datos y de los sistemas informáticos, protegiendo en general los intereses vinculados al desarrollo de las tecnologías de la información.

La totalidad de las disposiciones contenidas en el Convenio conservan como base la cooperación entre las Partes, lo cual es un desarrollo del tratamiento igualitario y los efectos recíprocos del Convenio. Destaca la Corte que lo contenido en este instrumento efectiviza los fines esenciales de la Constitución, atiende la soberanía e independencia del Estado colombiano en materia penal, y observa los mandatos constitucionales que se concretan con la adquisición de compromisos internacionales regidos por principios de conveniencia,

soberanía nacional, reciprocidad y equidad.

Asimismo, la Corte encuentra ajustado a la Constitución la disposición sobre la reserva anunciada por Colombia, mediante la Directora de Asuntos Jurídicos Internacionales del Ministerio de Relaciones Internacionales, como Estado Parte del Convenio sobre la Ciberdelincuencia, en el entendido que, por su intermedio, se propende por la defensa de los derechos fundamentales a la intimidad y al habeas data. La reserva a la que se acogerá el Estado colombiano, prevista en el numeral 3 del artículo 14 del Convenio, deberá ajustarse a los términos de la Constitución Política de 1991.

De conformidad con lo expuesto, la Corte Constitucional concluye que tanto el Convenio sobre la Ciberdelincuencia como su norma aprobatoria, Ley 1928 de 2018, son plenamente respetuosas de las disposiciones constitucionales colombianas.

VI. DECISIÓN

En mérito de lo expuesto, la Corte Constitucional de Colombia, en nombre del pueblo y por mandato de la Constitución,

RESUELVE

PRIMERO: Declarar EXEQUIBLE el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest, Hungría.

SEGUNDO: Declarar EXEQUIBLE la Ley 1928 de 2018, "por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de noviembre de 2001, en Budapest, Hungría".

Cópiese, notifíquese, comuníquese y cúmplase.

GLORIA STELLA ORTIZ DELGADO

Presidenta

CARLOS BERNAL PULIDO

Magistrado

Con aclaración de voto

DIANA FAJARDO RIVERA

Magistrada

LUIS GUILLERMO GUERRERO PÉREZ

Magistrado

ALEJANDRO LINARES CANTILLO

Magistrado

ANTONIO JOSÉ LIZARAZO OCAMPO

Magistrado

CRISTINA PARDO SCHLESINGER

Magistrada

JOSÉ FERNANDO REYES CUARTAS

Magistrado

ALBERTO ROJAS RÍOS

Magistrado

Secretaria General

ACLARACIÓN DE VOTO DEL MAGISTRADO

CARLOS BERNAL PULIDO

A LA SENTENCIA C-224/19

CONVENIO SOBRE LA CIBERDELINCUENCIA-Constitucionalidad de las obligaciones adquiridas por el Estado para tipificar ciertas conductas (Aclaración de voto)

CONVENIO SOBRE LA CIBERDELINCUENCIA-El convenio amplía los supuestos de la pornografía infantil (Aclaración de voto)

CONVENIO SOBRE LA CIBERDELINCUENCIA-Análisis del artículo sobre extradición (Aclaración de voto)

Expediente: LAT-455

Magistrada ponente: Cristina Pardo Schlesinger

Me permito presentar aclaración de voto en relación con la sentencia proferida por la Sala Plena en el asunto de la referencia. Si bien comparto el resolutivo, pues considero que prima facie no se advierte una contradicción de la ley, o del Convenio, con la Constitución Política, lo cierto es que el fundamento de la decisión debió incluir varios asuntos de relevancia constitucional:

1. Se debió analizar la constitucionalidad de las obligaciones adquiridas por el Estado colombiano en relación con el deber de tipificar ciertas conductas (artículos 2-12), dado que la salvaguarda del artículo 15 del Convenio sobre la Ciberdelincuencia no es aplicable a la sección 1, referida al derecho penal sustantivo. La jurisprudencia ha señalado que la asistencia judicial en materia penal es acorde con la Constitución[122] y que el Estado ejerce su soberanía al comprometerse internacionalmente a tipificar un delito[123]. Sin embargo, también ha dispuesto que la adopción de medidas para tipificar actos criminales comprendidos dentro del ámbito de un tratado se debe realizar con pleno respeto de la Constitución Política[124], pues, si el Estado asume la obligación de introducir modificaciones en su legislación, debe cumplir dicho compromiso sin falta, en virtud del principio de pacta sunt servanda[125]. Por todo lo anterior, la Corte debió evaluar si la obligación de introducir ciertos tipos penales al ordenamiento jurídico, que no está condicionada al respeto del derecho interno en virtud del Convenio, es susceptible de violar la Constitución[126]. En consecuencia, el análisis constitucional no se debió limitar a mencionar cuáles son los bienes jurídicos que se protegen con los tipos penales prescritos en el Convenio, sino que debió establecer si el contenido de las obligaciones es, prima

facie, constitucional, y cuáles son los parámetros de constitucionalidad que respaldan dicha conclusión.

2. El convenio amplía los supuestos de pornografía infantil. La Sala concluyó que el concepto de "pornografía infantil" del Convenio sobre la Ciberdelincuencia incorpora la definición del Protocolo Facultativo de la Convención Sobre los Derechos del Niño[127] suscrito por Colombia, sin embargo, la definición propuesta por el Convenio es más amplia que la dispuesta en el Protocolo. En efecto, se observa que la Convención incluye dentro de su definición una acepción no considerada ni en el Protocolo[128], ni en la definición actual del tipo penal en Colombia, esto es: "una persona que parezca un menor comportándose de una forma sexualmente explícita" (artículo 9, numeral 2, literal b). Con la adhesión al Convenio surge la obligación de tipificar esa conducta, por lo que dicho supuesto se debió someter a un análisis, al menos preliminar, de proporcionalidad y razonabilidad.

3. Se debió desarrollar el parámetro de constitucionalidad para el análisis del artículo 24 sobre extradición. Si bien el articulado del Convenio no contradice prima facie la disposición constitucional sobre extradición, y es posible aplicar a estos casos las salvaguardas de derecho interno señaladas en la sección 2 del Convenio[129], no se debió omitir que el artículo 35 superior constituye un parámetro específico para analizar la constitucionalidad de las obligaciones asumidas por el Estado colombiano relacionadas con esa figura. En particular, se debió retomar: (i) la prohibición expresa de extraditar por delitos políticos, (ii) la prohibición de extraditar cuando la solicitud se fundamenta en perseguir o castigar por razones discriminatorias, (iii) la exclusión de delitos cuya acción penal haya prescrito, (iv) la cláusula según la cual solo se pueden extraditar colombianos de nacimiento por delitos cometidos en el exterior, considerados como tal en la legislación colombiana[130].

4. Se debió precisar por qué fue válido el acto de sanción de la Ley 1928 de 2018. En el proyecto se explica que la Ministra de Educación sancionó la ley, en virtud de la delegación que le hizo el Presidente de la República por medio del Decreto 1255 del 19 de julio de 2018, a pesar de que el acto de delegación excluyó expresamente el numeral 2 del artículo 189 superior, referido a la dirección de "las relaciones internacionales". En ese sentido, la sentencia debió analizar si es válida la sanción de una ley que incorpora al ordenamiento jurídico colombiano un tratado internacional, cuando el delegatario de la función presidencial carece de la competencia para dirigir las relaciones internacionales. Lo anterior

tenía una relevancia especial en el caso sub examine, dado que el tratado se incorporó al ordenamiento jurídico por medio de la adhesión y, en consecuencia, la sanción de la ley constituía la manifestación concreta de la voluntad del Presidente de la República, como director de las relaciones internacionales, para obligar al Estado colombiano.

Fecha ut supra,

CARLOS BERNAL PULIDO

Magistrado

[1] La Corte Constitucional deja constancia que el texto del convenio que se revisa no corresponde a una versión oficial o autorizada en Colombia, sino a la traducción del Convenio hecha por el Reino de España, miembro de la Unión Europea. Lo anterior, al verificar, a folio 2 del cuaderno principal, que el tratado firmado y sometido a la aprobación del Congreso de la República es una versión en español; en esa medida, el texto de la Ley 1928 de 2018, contiene la siguiente manifestación: "Se adjunta copia fiel y completa del texto certificado en español del Convenio, certificado por la jefe de Área sw (sic) 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 de del (sic) Grupo Interno de Trabajo de Tratados y consta de dieciséis (16) folios". En efecto, el instrumento internacional objeto de análisis por parte de esta Corporación fue suscrito en inglés y francés; sin embargo, se aclara que dicha situación no es un aspecto que afecte la validez del mismo, pues se refiere a escenarios sobre su aplicación.

[2] Folios 82 al 86 del cuaderno principal.

[3] 24 de julio de 2018.

[4] Folios 117 al 120 del cuaderno principal.

[6] Folio 141 del cuaderno principal.

[7] Folio 142 del cuaderno principal.

[8] Folio 143 del cuaderno principal.

[9] Folio 98 del cuaderno principal.

[10] Folio 100 del cuaderno principal.

[11] Convenio sobre la Ciberdelincuencia, 23 de noviembre de 2001, Budapest, 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".

[12] Folio 101 del cuaderno principal.

[13] Convenio sobre la Ciberdelincuencia, 23 de noviembre de 2001, Budapest, artículo 9 – Delitos relacionados con la pornografía infantil:

"(…)

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

(…)

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.

(…)".

[14] Folio 105 del cuaderno principal.

[15] Concepto del 4 de septiembre de 2017, Estudio del Consejo Superior de Política Criminal al Proyecto de Ley número 058 de 2017 Senado "Por medio de la cual se aprueba el Convenio sobre la Ciberdelincuencia, adoptado el 25 de noviembre de 2001 en Budapest".

[16] Folio 153 del cuaderno principal.

[17] Folio 155.

[18] Ver entre otras, Corte Constitucional, Sentencias C–468 de 1997, C-378 de 1996, C-682 de 1996, C-400 de 1998, C-924 de 2000, C–576 de 2006 y C-332 de 2014.

[19] Artículo 154 de la Constitución Política.

[20] Artículo 157 de la Constitución Política.

[21] Artículo 160 de la Constitución Política.

[22] Artículo 241-10 de la Constitución Política.

[23] Corte Constitucional, Sentencias C–582 de 2002, C–933 de 2006, C–534 de 2008, C–537 de 2008, C–039 de 2009 y C–378 de 2009, entre otras.

[24] Folio 82 y siguientes del cuaderno principal.

[25] Folio 25 del cuaderno principal.

[26] Mediante la cual se examinó la constitucionalidad de la Ley Aprobatoria del "Acuerdo de promoción comercial entre la República de Colombia y los Estados Unidos de América´, sus ´cartas adjuntas´ y sus ´entendimientos´".

[27] Constitución Política, inciso final del artículo 154"Los proyectos de ley relativos a los tributos iniciarán su trámite en la Cámara de Representantes y los que se refieran a relaciones internacionales, en el Senado".(Subrayado fuera de texto)

[28] Constitución Política, artículo 241 "A la Corte Constitucional se le confía la guarda de la integridad y supremacía de la Constitución, en los estrictos y precisos términos de este

artículo. Con tal fin, cumplirá las siguientes funciones: (…) 10. Decidir definitivamente sobre la exequibilidad de los tratados internacionales y de las leyes que los aprueben. Con tal fin, el Gobierno los remitirá a la Corte, dentro de los seis días siguientes a la sanción de la ley. Cualquier ciudadano podrá intervenir para defender o impugnar su constitucionalidad. Si la Corte los declara constitucionales, el Gobierno podrá efectuar el canje de notas; en caso contrario no serán ratificados. Cuando una o varias normas de un tratado multilateral sean declaradas inexequibles por la Corte Constitucional, el Presidente de la República sólo podrá manifestar el consentimiento formulando la correspondiente reserva".

[29] Cfr. Folios 1 a 20 del cuaderno 1. En la GC 631 del 1 de agosto de 2017, se pueden consultar las páginas 13 a 36.

[30] Constitución Política, artículo 157 "Ningún proyecto será ley sin los requisitos siguientes: 1. Haber sido publicado oficialmente por el Congreso, antes de darle curso en la comisión respectiva. (…)".

[31] Ley 5 de 1992, artículo 156. "Presentación y publicación de la ponencia. El informe será presentado por escrito, en original y dos copias, al secretario de la Comisión Permanente. Su publicación se hará en la Gaceta del Congreso dentro de los tres (3) días siguientes. // Sin embargo, y para agilizar el trámite del proyecto, el Presidente podrá autorizar la reproducción del documento por cualquier medio mecánico, para distribuirlo entre los miembros de la Comisión; ello, sin perjuicio de su posterior y oportuna reproducción en la Gaceta del Congreso".

[32] Ver folios 18 a 20 del cuaderno de pruebas No. 1.

[33] Ley 5 de 1992, artículo 157 "Iniciación del debate. La iniciación del primer debate no tendrá lugar antes de la publicación del informe respectivo.// No será necesario dar lectura a la ponencia, salvo que así lo disponga, por razones de conveniencia, la Comisión.// El ponente, en la correspondiente sesión, absolverá las preguntas y dudas que sobre aquélla se le formulen, luego de lo cual comenzará el debate.// Si el ponente propone debatir el proyecto, se procederá en consecuencia sin necesidad de votación del informe. Si se propone archivar o negar el proyecto, se debatirá esta propuesta y se pondrá en votación al cierre del debate.// Al debatirse un proyecto, el ponente podrá señalar los asuntos fundamentales acerca de los cuales conviene que la Comisión decida en primer término".

[34] http://svrpubindc.imprenta.gov.co/senado/view/gestion/gacetaPublica.xhtml

[35] Ver folio 41 del cuaderno de pruebas No. 1.

[36] Ver folios 43 a 64 del cuaderno de pruebas No. 1.

[37] Ver folios 62 al 64 del cuaderno No. 1.

[38] Ver folios 1 y 2 del cuaderno de pruebas No. 1.

[39] Ver folios 45 a 54 del cuaderno principal.

[40] http://svrpubindc.imprenta.gov.co/senado/view/gestion/gacetaPublica.xhtml

[41] CD, folio 54 del cuaderno principal.

[42] Folio54 del cuaderno principal.

[44] Ver folio 54 del cuaderno principal.

[45] Ver folio 67 del cuaderno de pruebas No. 1.

[46] Ver folio 941 del cuaderno de pruebas No. 1.

[47] Ver folio 95 del cuaderno de pruebas No. 1.

[48] Ver folios 69 a 86 del cuaderno de pruebas No. 1.

[49] Ver folio 116 del cuaderno de pruebas No. 1.

[50] Ver folios 80 y siguientes del cuaderno de pruebas No. 1.

[51] Folio 116 del cuaderno de pruebas No. 1.

[52] Folio 116 del cuaderno de pruebas No. 1, (CD).

[53] Folio 28 del cuaderno principal.

[54] Folio 1 del cuaderno de pruebas No. 1.

[55] Folios 86 del cuaderno principal.

[56] Ver folio 1 del cuaderno de principal.

[57]Gaceta del Congreso No.631 del 1 de agosto de 2017.

[58] Publicación de la ponencia para primer debate en la Gaceta del Congreso No. 771 del 11 de septiembre de 2017.

[59] Constitución Política, artículo 157, numeral 2 "Haber sido aprobado en primer debate en la correspondiente comisión permanente de cada Cámara. El reglamento del Congreso determinará los casos en los cuales el primer debate se surtirá en sesión conjunta de las comisiones permanentes de ambas Cámaras".

[60] Constitución Política, artículo 157, numeral 3 "Haber sido aprobado en cada Cámara en segundo debate".

[61] Constitución Política, artículo 157, numeral 4 "Haber obtenido la sanción del Gobierno".

[62] Según consta en el Acta No. 08 de esa fecha, publicada en la Gaceta del Congreso No. 1184 del 12 de diciembre de 2017.

[63] Según consta en la Gaceta del Congreso No. 118 del 10 de abril de 2018.

[64] Según consta en el Acta No. 26 del 17 de mayo de 2017, publicada en la Gaceta del Congreso No. 401 del 8 de junio de 2018.

[65] Según consta en el Acta de Plenaria No. 296 de la sesión del de junio 20 de 2018, publicada en la Gaceta del Congreso No. 498 del 5 de julio de 2018.

[66]"Por el cual se adopta una Reforma Política constitucional y se dictan otras disposiciones"

[67] Cfr. Sentencia C-644 de 2004.

[68] Cfr. Auto 038 de 2004 y Sentencia C-533 de 2004.

[70] http://svrpubindc.imprenta.gov.co/senado/view/gestion/gacetaPublica.xhtml

[71] http://svrpubindc.imprenta.gov.co/senado/view/gestion/gacetaPublica.xhtml

[72]"Por la cual se expide el Reglamento del Congreso; el Senado y la Cámara de Representantes"

[73] http://conventions.coe.int/Treaty/Commun

[74] Listados de firmas y tarificaciones del Convenio de Budapest, página web oficial del Consejo de Europa. https://www.coe.int/es/web/compass/council-of-europe

[75] Minuta de la Biblioteca del Congreso Nacional Verona Barrios Achavar, vbarrios@bcn. Anexo Santiago 1984, Valparaíso 3179. Asesoría Técnica Parlamentaria. Área Gobierno. Defensa Y relaciones Internacionales. 29/09/2014. https://www.bcn.cl/

[76] Convenio sobre la ciberdelincuencia, preámbulo, folio 7 del cuaderno de pruebas número 1.

[77] XXI Conferencia, Praga, 10 y 11 de junio de 1997.

[78] Adoptada en la XXIII Conferencia de Ministro de Justicia europeos, Londres, 8 y 9 de junio de 2000.

[79] Segunda Cumbre, Estrasburgo, 10 y 11 de octubre de 1997.

[80] Artículo 4, numeral 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 informativos.

[81] Sentencia C-748 de 2011.

[82] "Artículo2:

A los efectos del presente Protocolo:

a) Por venta de niños se entiende todo acto o actuación en virtud del cual un niño es transferido por una persona o grupo de personas a otra a cambio de remuneración o de

cualquier otra retribución;

b) Por prostitución infantil se: entiende la utilización de un niño en actividades sexuales a cambio de remuneración o cualquier otra retribución;

c) Por pornografía infantil se entiende toda presentación, por cualquier medio, de un niño dedicado a actividades sexuales explicitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales". (resaltado agregado).

[83] Constitución Política de 1991, "Artículo 61. El Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley".

[84] Sentencia C-148 de 2015.

[85] Reiterada en Sentencia T-030 de 2017.

[86] Ibídem.

[87] Según la exposición de motivos del proyecto de ley número 58 de 2017 Senado, publicado en la Gaceta del Congreso 631 del 1 de agosto de 2017, página 33.

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 adoptar· 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.

[89] Gaceta del Congreso 631 del 1 de agosto de 2017, página 33.

[90] En la citada providencia, la Sala Plena de la Corte constitucional requirió a la la Directora de Asuntos Jurídicos Internacionales del Ministerio de Relaciones Exteriores para que remitiera a esta Corporación y con destino al proceso de la referencia, copia del proyecto de la reserva anunciada en el numeral III de la exposición de motivos del Proyecto de ley "Por medio de la cual se aprueba el Convenio sobre la Ciberdelincuencia, adoptado el 25 de noviembre de 2001 en Budapest".

[91] Sentencia C-640 de 2010.

[92] Sentencias T-787 de 2004, T-634 de 2013 y T-050 de 2016.

[93] Reiterada, entre otras, en las Sentencias T-015 del 2015 y T-050 de 2016.

[94] Sentencia T-696 de 1996.

[95] Sentencia T-117 de 2018.

[96] Sentencia T-050 de 2016.

[97] Artículo 15. El artículo 235 de la Ley 906 de 2004, Código de Procedimiento Penal, quedará así:

Artículo 235. Interceptación de comunicaciones telefónicas y similares. El fiscal podrá

ordenar, con el objeto de buscar elementos materiales probatorios, evidencia física, búsqueda y ubicación de imputados o indiciados, que se intercepten mediante grabación magnetofónica o similares las comunicaciones telefónicas, radiotelefónicas y similares que utilicen el espectro electromagnético, cuya información tengan interés para los fines de la actuación. En este sentido, las entidades encargadas de la operación técnica de la respectiva interceptación tienen la obligación de realizarla inmediatamente después de la notificación de la orden.

En todo caso, deberá fundamentarse por escrito. Las personas que participen en estas diligencias se obligan a guardar la debida reserva.

Por ningún motivo se podrán interceptar las comunicaciones del defensor.

La orden tendrá una vigencia máxima de tres (3) meses, pero podrá prorrogarse hasta por otro tanto si, a juicio del fiscal, subsisten los motivos fundados que la originaron.

[98] "Por medio de la cual se reforman parcialmente las Leyes 906 de 2004, 599 de 2000 y 600 de 2000 y se adoptan medidas para la prevención y represión de la actividad delictiva de especial impacto para la convivencia y seguridad ciudadana".

[99] Artículo 52. Interceptación de comunicaciones. Reglamentado por el Decreto Nacional 1704 de 2012. El artículo 235 de la Ley 906 de 2004 quedará así:

Artículo 235. Interceptación de comunicaciones. El fiscal podrá ordenar, con el objeto de buscar elementos materiales probatorios, evidencia física, búsqueda y ubicación de imputados, indiciados o condenados, que se intercepten mediante grabación magnetofónica o similares las comunicaciones que se cursen por cualquier red de comunicaciones, en donde curse información o haya interés para los fines de la actuación. En este sentido, las autoridades competentes serán las encargadas de la operación técnica de la respectiva interceptación así como del procesamiento de la misma. Tienen la obligación de realizarla inmediatamente después de la notificación de la orden y todos los costos serán a cargo de la autoridad que ejecute la interceptación.

En todo caso, deberá fundamentarse por escrito. Las personas que participen en estas diligencias se obligan a guardar la debida reserva.

Por ningún motivo se podrán interceptar las comunicaciones del defensor.

La orden tendrá una vigencia máxima de seis (6) meses, pero podrá prorrogarse, a juicio del fiscal, subsisten los motivos fundados que la originaron.

La orden del fiscal de prorrogar la interceptación de comunicaciones y similares deberá someterse al control previo de legalidad por parte del Juez de Control de Garantías.

[100] "Por medio de la cual se reforma el Código Penal, el Código de Procedimiento Penal, el Código de Infancia y Adolescencia, las reglas sobre extinción de dominio y se dictan otras disposiciones en materia de seguridad".

[101] "Artículo 14. Intimidad. Toda persona tiene derecho al respeto de su intimidad. Nadie podrá ser molestado en su vida privada.

No podrán hacerse registros, allanamientos ni incautaciones en domicilio, residencia, o lugar de trabajo, sino en virtud de orden escrita del Fiscal General de la Nación o su delegado, con arreglo de las formalidades y motivos previamente definidos en este código. Se entienden excluidas las situaciones de flagrancia y demás contempladas por la ley.

De la misma manera deberá procederse cuando resulte necesaria la búsqueda selectiva en las bases de datos computarizadas, mecánicas o de cualquier otra índole, que no sean de libre acceso, o cuando fuere necesario interceptar comunicaciones. Texto subrayado declarado EXEQUIBLE por la Corte Constitucional mediante Sentencia C-336 de 2007, en el entendido que se requiere de orden judicial previa cuando se trata de los datos personales, organizados con fines legales y recogidos por instituciones o entidades públicas o privadas debidamente autorizadas para ello.

En estos casos, dentro de las treinta y seis (36) horas siguientes deberá adelantarse la respectiva audiencia ante el juez de control de garantías, con el fin de determinar la legalidad formal y material de la actuación."

[102] "Artículo 154. Modificado por el 12 de la Ley 1142 de 2007. Modalidades. Se tramitará en audiencia preliminar:

1. El acto de poner a disposición del juez de control de garantías los elementos recogidos en

registros, allanamientos e interceptación de comunicaciones ordenadas por la Fiscalía, para su control de legalidad dentro de las treinta y seis (36) horas siguientes.

2. La práctica de una prueba anticipada.

3. La que ordena la adopción de medidas necesarias para la protección de víctimas y testigos.

4. La que resuelve sobre la petición de medida de aseguramiento.

5. La que resuelve sobre la petición de medidas cautelares reales.

6. La formulación de la imputación.

7. El control de legalidad sobre la aplicación del principio de oportunidad.

8. Las peticiones de libertad que se presenten con anterioridad al anuncio del sentido del fallo.

9. Las que resuelven asuntos similares a los anteriores."

[103] Artículo 237. Audiencia de control de legalidad posterior. Modificado por el art. 16, Ley 1142 de 2007. Dentro de las veinticuatro (24) horas siguientes al diligenciamiento de las órdenes de registro y allanamiento, retención de correspondencia, interceptación de comunicaciones o recuperación de información dejada al navegar por internet u otros medios similares, el fiscal comparecerá ante el juez de control de garantías, para que realice la audiencia de revisión de legalidad sobre lo actuado.

Durante el trámite de la audiencia sólo podrán asistir, además del fiscal, los funcionarios de la policía judicial y los testigos o peritos que prestaron declaraciones juradas con el fin de obtener la orden respectiva, o que intervinieron en la diligencia. El texto subrayado fue declarado INEXEQUIBLE por la Corte Constitucional mediante Sentencia C-025 de 2009. El resto del inciso fue declarado EXEQUIBLE en la misma Sentencia, siempre que se entienda, dentro del respeto a la naturaleza de cada una de las etapas estructurales del procedimiento penal acusatorio, que cuando el indiciado tenga noticia de que en las diligencias practicadas en la etapa de indagación anterior a la formulación de la imputación,

se está investigando su participación en la comisión de un hecho punible, el juez de control de garantías debe autorizarle su participación y la de su abogado en la audiencia posterior de control de legalidad de tales diligencias, si así lo solicita.

El juez podrá, si lo estima conveniente, interrogar directamente a los comparecientes y, después de escuchar los argumentos del fiscal, decidirá de plano sobre la validez del procedimiento.

[104] El artículo 1º del Decreto 1704 de 2012 al definir la interceptación de las comunicaciones, dispuso que se trata de un mecanismo de seguridad pública que busca optimizar la labor de investigación de los delitos que adelantan las autoridades y organismos competentes, en el marco de la Constitución y la ley.

[105] Modificado por el artículo 16 de la Ley 1142 de 2007.

[106] "Por medio de la cual se reforma el Código Penal, el Código de Procedimiento Penal, el Código de Infancia y Adolescencia, las reglas sobre extinción de dominio y se dictan otras disposiciones en materia de seguridad"

[107] El Decreto 1900 de 1990 establece la regulación del servicio público de telecomunicaciones. El artículo 9 dispone lo siguiente:

Artículo 9º. El Estado garantiza como derecho fundamental de la persona la intimidad individual y familiar contra toda intromisión en ejercicio de actividades de telecomunicaciones que no corresponda al cumplimiento de funciones legales.

[108] "Por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones".

[109] Demanda de inconstitucionalidad propuesta contra los artículos 3, 4, 5, 7, 8, 9, 14 y 16 de la Ley 228 de 1995 "Por la cual se determina el régimen aplicable a las contravenciones especiales y se dictan otras disposiciones".

[110] "Por la cual se regula la tenencia y registro de perros potencialmente peligrosos."

[111] Mediante la cual se juzgó la constitucionalidad de algunos apartes del artículo 237 de la Ley 906 de 2004.

[112] Demanda de inconstitucionalidad promovida contra el Artículo 52 (parcial) de la Ley 1453 de 2011 "por medio de la cual se reforma el Código Penal, el Código de Procedimiento Penal, el Código de Infancia y Adolescencia, las reglas sobre extinción de dominio y se dictan otras disposiciones en materia de seguridad".

[113] Caso en que se alegaba la vulneración de los derechos fundamentales a la intimidad, al debido proceso y al acceso a la administración de justicia del accionante por la configuración de un defecto fáctico en el trámite del proceso que cursó en la Sala de Casación Penal de la Corte Suprema de Justicia, autoridad judicial que valoró como parte de la actividad probatoria, pruebas trasladadas consistentes en comunicaciones telefónicas conocidas por la Procuraduría General de la Nación en desarrollo de un proceso disciplinario, mediante actividad de policía judicial.

[114] "Por la cual se dictan disposiciones generales para la protección de datos personales".

[115] T-811 de 2010.

[116] T-198 de 2015.

[117] Sentencias T-718 de 2005 y C-1011 de 2008.

[118] Código Penal, artículo 100. Comiso. "Los instrumentos y efectos con los que se haya cometido la conducta punible o que provengan de su ejecución, y que no tengan libre comercio, pasarán a poder de la Fiscalía General de la Nación o a la entidad que ésta designe, a menos que la ley disponga su destrucción.

Igual medida se aplicará en los delitos dolosos, cuando los bienes, que tengan libre comercio y pertenezcan al responsable penalmente, sean utilizados para la realización de la conducta punible, o provengan de su ejecución.

En las conductas culposas, los vehículos automotores, naves o aeronaves, cualquier unidad montada sobre ruedas y los demás objetos que tengan libre comercio, se someterán a los

experticios técnicos y se entregarán provisionalmente al propietario, legítimo tenedor salvo que se haya solicitado y decretado su embargo y secuestro. En tal caso, no procederá la entrega, hasta tanto no se tome decisión definitiva respecto de ellos.

La entrega será definitiva cuando se garantice el pago de los perjuicios, se hayan embargado bienes del sindicado en cuantía suficiente para atender al pago de aquellos, o hayan transcurrido diez y ocho (18) meses desde la realización de la conducta, sin que se haya producido la afectación del bien".

[119] Sentencia C-621 de 2001.

[120] "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".

[121] El Convenio sobre la ciberdelincuencia refiere como elementos complementarios la producción, importación, introducción, venta, difusión, alteración, borrado o supresión de datos informáticos mediante la utilización de sistemas informáticos, programas informáticos, contraseñas, códigos de acceso o dispositivos para la comisión de cualquiera de los delitos consagrados en los artículos 2 al 5 del Tratado.

[122] Sentencia C-405 de 1999.

[123] Sentencia C-1055 de 2003.

[124] Sentencia C-1055 de 2003.

[125] Sentencia C-405 de 2004.

[126] Sentencia C-176 de 1994.

[127] Aprobado por la Ley 765 de 2000, la cual fue declarada exequible por la Corte en la

Sentencia C-318 de 2003.

[128] Artículo 2, literal C: “Por pornografía infantil se entiende toda representación, por cualquier medio, de un niño dedicado a actividades sexuales explícitas, reales o simuladas, o toda representación de las partes genitales de un niño con fines primordialmente sexuales”.

[129] Convenio sobre la Ciberdelincuencia, artículos 15 y 24, numeral 5.

[130] Sentencia C-333 de 2014.