EL CONVENIO DE BUDAPEST: UN ANÁLISIS DESDE EL ORDENAMIENTO JURÍDICO COLOMBIANO

CARLOS DANIEL MOLINA DÍAZ

UNIVERSIDAD PONTIFICIA BOLIVARIANA

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

DERECHO

MEDELLÍN

2021

EL CONVENIO DE BUDAPEST: UN ANÁLISIS DESDE EL ORDENAMIENTO JURÍDICO COLOMBIANO

CARLOS DANIEL MOLINA DÍAZ

Trabajo de Grado para optar al título de abogado

ASESORA:

KENYA LORENA GÓMEZ URREA

Pregrado en Derecho

Escuela de Derecho y Ciencias Políticas

Universidad Pontificia Bolivariana

2.021

Declaración de Originalidad

Fecha: 28 de junio de 2021

Nombre del estudiante: Carlos Daniel Molina Díaz

Declaro que este trabajo de grado no ha sido presentado con anterioridad para optar a un título, ya sea en igual forma o con variaciones, en esta o en cualquiera otra universidad.

Declaro, asimismo, que he respetado los derechos de autor y he hecho uso correcto de las normas de citación de fuentes, con base en lo dispuesto en las normas de publicación previstas en los reglamentos de la Universidad.

CARLOS DANIEL MOLINA DÍAZ

C.C. 1.017.242.102

ID: 000307374

DEDICATORIA.

A mi familia, quienes han sido mi luz y soporte.

A mi asesora, por su acompañamiento y dirección.

A mis amigos por la motivación.

EL CONVENIO DE BUDAPEST: UN ANÁLISIS DESDE EL ORDENAMIENTO JURÍDICO COLOMBIANO

THE BUDAPEST CONVENTION: AN ANALYSIS FROM THE COLOMBIAN LEGAL SYSTEM

SUMARIO:

Introducción…… 6

I. Sobre la Ciberdelincuencia……... 7

1.1. Contexto Histórico…….. 7

II. El Convenio de Budapest…… 9

2.1. Capítulo I – Terminología……..10

2.2. Capitulo II – Medidas que deberán de adoptarse a nivel nacional.11

2.3. Capítulo III – Cooperación Internacional……..…13

2.4. Capítulo IV – Cláusulas Finales……14

III. Regulación en Colombia……..16

3.1. Marco Normativo……16

3.2. Contexto Nacional…….. 23

IV. Del Control de Constitucionalidad……..25

4.1. Sentencia C-224/19……25

4.1.2. Análisis Formal…….26

4.1.3. Análisis Material……28

V. Conclusiones……..31

VI. Referencias……32

RESUMEN:

En el presente trabajo, se hará un análisis sobre El Convenio de Budapest y su regulación en Colombia. Para ello, en primer lugar, se efectuará un estudio del referido convenio, abarcando el contexto histórico sobre el cual se erige hasta las disposiciones regulatorias del mismo; En segundo lugar se realizará un análisis sobre cómo se ha regulado la Ciberdelincuencia en Colombia, desde los proyectos de ley que pretendían regular la materia, cruzando por la ley que modificó el Código Penal al introducir un nuevo bien jurídico dentro de nuestro ordenamiento, concerniente a la protección de la información y de los datos contenidos en el ciberespacio, se realiza un estudio respecto de la ley aprobatoria del referido convenio y con base en lo anterior se concluye con el estudio de constitucionalidad efectuado por la Corte Constitucional respecto de la norma aprobatoria del Convenio de Budapest.

PALABRAS CLAVE: *Convenio de Budapest, Ciberdelincuencia, Ordenamiento Jurídico, Protección de la información y de los datos, Derecho Penal*

ABSTRACT:

In the following paper, an analysis will be made about The Budapest Convention and its regulation regarding the Colombian legal system, starting the exposition from the Convention of Budapest, which is the international instrument of excellence which regulates the subject. In the first place a study of the convention will be made, from the historic context to the regulatory dispositions of it; In second place an analysis will be made about how Cybercrime has been regulated in Colombia, from the prospects of law which intended to regulate the subject, to the law which modify the Penal Code, and the study regarding the law of approval of the Convention, to finally wrapped it up by doing a scrutiny of the Constitutional Control made by the court in relation to the convention and the internal legal system

KEY WORDS:

Convention of Budapest, Cybercrime, Legal System, Protection of information and data, Criminal Law

INTRODUCCIÓN:

El presente trabajo de grado tiene por objeto de estudio El Convenio de Budapest y su regulación dentro del ordenamiento jurídico colombiano. A lo largo de este se abordarán temáticas tales como los orígenes de la protección de los datos por medio del *Convenio sobre la Ciberdelincuencia de Budapest* y cómo ha sido su legislación en Colombia, desde la creación de un nuevo bien jurídico (ley 1273/09).

Para los efectos pertinentes el presente trabajo se puede entender en dos secciones macro: la primera abarca las temáticas relacionadas al convenio de Budapest, como el contexto histórico dentro del cual surge el mismo, abordando de esta forma el porqué de este instrumento jurídico internacional, y a reglón seguido se realiza una síntesis de los capítulos que integran el articulado. Una segunda parte que trata las temáticas concernientes a la regulación de los delitos *Cibernéticos* en Colombia, para este cometido se inicia haciendo referencia al marco normativo que ha regulado la materia dentro del país, abarcando las siguientes: los proyectos de ley pioneros en la materia; la creación y posterior incorporación de un bien jurídico que modificó el Código Penal (ley 1273 del 2.009); sobre la ley aprobatoria del referido convenio (ley 1928 del 2.018) y el control de constitucionalidad realizado por la Corte Constitucional para la debida incorporación en nuestro ordenamiento. (Sentencia C-224/19).

Con la emergencia sanitaria que nos ha golpeado a lo largo del último año se ha evidenciado la dependencia casi que total que se tiene con los medios informáticos al igual que con los datos nuestros que reposan en el ciberespacio. Es claro que hoy en día no existe aspecto de las personas que no involucre trato con una herramienta virtual, toda vez que por medio de estas nuevas tecnologías se logra un fácil y rápido acceso a los datos contenidos en los sistemas informáticos. Estas nuevas tecnologías son un desafío para la realidad fenoménica de nuestra sociedad, de forma tal que es menester y obligación del campo jurídico comprender las mismas para así proteger a las personas de los peligros de estas, siendo esa la motivación y fuente de interés para el presente trabajo.

I. SOBRE LA CIBERDELINCUENCIA: "EL CONVENIO DE BUDAPEST."

1.1. CONTEXTO HISTÓRICO.

En noviembre de 1.996, el Comité Europeo para los Problemas Criminales (CDPC[1]) decide establecer un comité de expertos, al que se le encomendaría la labor de enfocarse netamente en los delitos informáticos, puesto que para aquel entonces los mismos estaban en un auge en razón a las tecnologías emergentes, y frente a esto los ordenamientos jurídicos europeos no se encontraban preparados para regular las eventualidades con las que venían tales tecnologías. Por tanto, el mandato para tal comité fue examinar la delincuencia relacionada con la informática y las cuestiones de procedimiento penal vinculadas a la tecnología de la información, en particular los siguientes temas:

1. Los delitos cometidos en el ciberespacio.
2. Cuestiones del derecho penal sustantivo que merecían un enfoque común permeado por la cooperación internacional
3. El uso; entendido como la posibilidad de uso transfronterizo y la aplicabilidad de los poderes coercitivos en un entorno tecnológico.
4. La Jurisdicción; la necesidad de determinar dónde se cometió el delito y por tanto qué norma o normas se habría de aplicar para la persecución de este.
5. Cuestiones relativas a la cooperación internacional.

Dentro de las labores del CDPC se encontraba la de elaborar informes, pero estos eran insuficientes para dichas eventualidades, y por tanto se percataron de que únicamente un instrumento internacional de carácter vinculante podría asegurar la

[1] Constituido en 1958, el Comité Europeo para los Problemas Criminales (CDPC por sus siglas en ingles *"European Committee on Crime Problems"*) le fue confiada por el Comité de Ministros, la responsabilidad para supervisar y coordinar las actividades del Consejo de Europa en el campo para la prevención del crimen y el control del crimen. El CDPC se reúne en la sede del Consejo de Europa que se encuentra en Estrasburgo Francia.
El CDPC identifica las prioridades para la cooperación Legal Intergubernamental, hace y presenta propuestas al Comité de Ministros respecto de las actividades que se dan en los campos del derecho penal (sustancial y procesal), criminología y la penología, para luego implementar tales propuestas.
El CDPC también elabora convenciones, recomendaciones y reportes. De forma tal que organiza y prepara congresos de investigación criminológica al igual que coloquios criminológicos encaminados a perfeccionar la política criminal.

eficacia necesaria en la lucha contra estos fenómenos virtuales, de forma tal que el derecho penal pudiese estar al tanto de estos desarrollos tecnológicos, ya que estos ofrecen incontables oportunidades para hacer un uso indebido de las facilidades del ciberespacio y perjudicar así intereses legítimos.

Por lo anterior, el CDPC, le encomendó al Profesor H.W.K KASPERSEN[2] que elaborara un informe donde se plasmaran los riesgos y acciones por tomar respecto de la emergente ciberdelincuencia, en tal encomienda se llegó a la conclusión de que era imperante la implementación de un convenio internacional que abordara cuestiones tanto sustanciales como procesales del derecho penal internacional que permitiesen regular los delitos cibernéticos.

Impulsados y motivados por el informe del profesor KASPERSEN, fue que en diciembre del año 1.996, el CDPC decide crear un nuevo comité que fue denominado *"Comité de Expertos en la Delincuencia del Ciberespacio" (PC -CY; por sus siglas en Ingles).*

El aludido Comité de Expertos en la Delincuencia del Ciberespacio (PC-CY) inició sus labores formalmente en abril de 1.997, cuando comenzó a llevar a cabo negociaciones para un proyecto de un convenio internacional para regular la ciberdelincuencia.

Inicialmente debían terminar para el 31 de diciembre de 1.999 pero para ese entonces el Comité no se encontraba en posición de concluir a plenitud las negociaciones respecto de ciertas cuestiones incluidas en el proyecto del convenio y por tanto sus términos iniciales se prorrogaron hasta el 31 de diciembre del año 2.000, luego de una decisión[3] del Consejo de Ministros de Justicia Europeos[4], donde daban su aval y apoyo a las actuaciones del PC-CY.

---

[2] Henrik Wijnandus Kristian Kaspersen experto en Derecho informático de la Universidad de Ámsterdam

[3] Decisión Núm. CM/DEL/DEC (99) 679

[4] Es el principal órgano legislativo y de toma de decisiones de la Unión Europea, tiene la responsabilidad de aprobar las leyes y adoptar las decisiones políticas. También es el máximo responsable de la Política Exterior y de Seguridad Común (PESC), de forma tal que los Gobiernos trabajan uniendo fuerzas y esfuerzos para manifestarse como una sola voz respecto de las cuestiones de política exterior, siendo asistidos por el Alto Representante para la Política Exterior y de Seguridad Común, el Dr. JAVIER SOLANA.

- Entre abril de 1.997 y diciembre del 2.000 tuvieron lugar diez reuniones plenarias del Comité PC-CY y 15 reuniones de su grupo de redacción.
- En abril del 2.000 se publicó la primera versión del proyecto, esto con miras a que los estados negociadores pudiesen efectuar consultas internas respecto de este, lo cual fue de gran utilidad y aplaudido por los estados parte.
- En octubre del 2.000, el Comité de Ministros Europeos solicitó a la Asamblea Parlamentaria[5] que emitiera un dictamen sobre el proyecto del convenio.
- Luego de ser finalizado el proyecto del Convenio, fue revisado en conjunto con su memorando explicativo, los cuales fueron sometidos al CDPC durante su 50ª sesión plenaria llevada a cabo en Junio de 2.001 para su aprobación inicial.
- Luego de obtener el visto bueno por parte del CDPC, fue remitido al Consejo de Ministros Europeos para su debida aprobación, quedando así listo para su firma por parte de los estados miembros de la Unión Europea, demás interesados e invitados.

II. EL CONVENIO

El convenio tiene tres finalidades primordiales:

I. La primera es la de concertar los elementos de las conductas desviadas de acuerdo con el derecho penal sustantivo de cada nación y de igual forma buscar armonizar los diferentes preceptos vinculados a la materia de delitos informáticos de cada país.

II. En segundo lugar, se encuentra, el instaurar de forma acorde al derecho penal procesal de cada estado, los poderes, atribuciones y demás facultades que resulten necesarias para la debida investigación y posterior procesamiento de tales delitos cibernéticos, también para las demás

[5] La Asamblea Parlamentaria reúne a 324 parlamentarios de los 47 Estados miembros. Elige al Secretario General, al Comisario de Derechos Humanos y a los jueces del Tribunal Europeo de Derechos Humanos. Ofrece un foro democrático para el debate y lleva a cabo misiones de observación de elecciones. Sus comisiones desempeñan un papel importante en el examen de las cuestiones de actualidad.

conductas delictivas que se cometan por medio del uso de un sistema informático y para las demás pruebas conexas que se encuentren en formato electrónico.

III. En tercer y último lugar, el convenio propende por implantar un régimen que sea tan rápido como eficaz para lograr una debida y correcta cooperación internacional que permita investigar y procesar los delitos cibernéticos de forma oportuna.

Es en razón a tales finalidades primordiales que el convenio encuentra su lógica y estructura, misma que se encuentra fragmentada en cuatro capítulos, siendo tales:

A. TERMINOLOGÍA
B. MEDIDAS QUE DEBERÁN ADOPTARSE A NIVEL NACIONAL
    - El derecho penal sustantivo.
    - El derecho penal procesal.
C. COOPERACIÓN INTERACIONAL
D. CLÁUSULAS FINALES

2.1. CAPÍTULO I - TERMINOLOGÍA

El Comité de Expertos en la Delincuencia del Ciberespacio (PC-CY), entendieron al momento de redactar el Convenio de Budapest, que los estados parte no tendrían la obligación de copiar al tenor literal los cuatro conceptos traídos en el artículo 1º de dicho convenio, dentro de su ordenamiento jurídico.

La obligación que contraían era que dentro de su regulación interna abarcaran tales conceptos de forma coherente con los principios del convenio y que de igual manera consagraran un margen idéntico para su implementación; tales conceptos son:

CONCEPTO	DEFINICIÓN
SISTEMA INFORMÁTICO	*"Por sistema informático se entenderá todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa;"*

DATOS INFORMÁTICOS	*"Por datos informáticos se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función;"*
PROVEEDOR DE SERVICIOS	*"Por proveedor de servicios se entenderá:* *i. Toda entidad publica o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático, y* *ii. Cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo;"*
DATOS RELATIVOS AL TRÁFICO	*"Por datos relativos al tráfico se entenderá todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente"*

**TABLA*[6]*

2.2. CAPÍTULO II – MEDIDAS QUE DEBERÁN ADOPTARSE A NIVEL NACIONAL.

SECCIÓN I – DERECHO PENAL SUSTANTIVO.

Este acápite del convenio engloba las disposiciones concernientes a las conductas delictivas y demás preceptos ligados, correspondiente a la esfera de la ciberdelincuencia. De forma tal que se limita a dar la definición de las conductas delictivas que se regularán a través del aludido convenio, conductas que son congregadas dentro de cuatro categorías diferentes, a saber:

[6] Convenio sobre la ciberdelincuencia, Articulo 1° - Definiciones, Capítulo I – Terminología. (2001), Budapest, Noviembre 23

- Titulo 1 – Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:
    - Art 2 – Acceso Ilícito
    - Art 3 - Interceptación ilícita
    - Art 4 – Ataques a la integridad de los datos
    - Art 5 – Ataques a la integridad del sistema
    - Art 6 – Abuso de los dispositivos
- Titulo 2 – Delitos informáticos
    - Art 7 – Falsificación informática
    - Art 8 – Fraude informático
- Titulo 3 – Delitos relacionados con el contenido
    - Art 9 – Delitos relacionados con la pornografía infantil
- Titulo 4 – Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines
    - Art 10 – Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

SECCIÓN II – DERECHO PENAL PROCESAL

En este acápite se avanza más allá de los delitos definidos con anterioridad toda vez que se emplea para cualquier conducta delictiva, siempre y cuando tal comportamiento sea cometido a través de un sistema informático, también se utiliza para las pruebas que se encuentren en formato electrónico, plasmando así el ámbito de aplicación de las disposiciones de procedimiento dentro de los preceptos comunes para el mismo.

De igual forma se regulan aquí las condiciones y salvaguardas que se han de emplear para todas las potestades procesales que integran este capítulo, y a reglón seguido se decretan los poderes procesales para regular tales actuaciones dividiendo dichas facultades por títulos, siendo estas:

- Título 2 – Conservación rápida de datos informáticos almacenados
    - Art 16 – Conservación rápida de datos informáticos almacenados

- Art 17 – Conservación y revelación parcial rápidas de datos relativos al tráfico

- Título 3 – Orden de presentación
  - Art 18 – Orden de presentación
- Título 4 – Registro y confiscación de datos informáticos almacenados
  - Art 19 – Registro y confiscación de datos informáticos almacenados
- Título 5 – Obtención en tiempo real de datos informáticos
  - Art 20 – Obtención en tiempo real de datos relativos al tráfico
  - Art 21 – Interceptación de datos relativos al contenido

SECCIÓN III – JURISDICCIÓN

En este acápite se señala las temáticas relativas a la jurisdicción, donde se dice que cada parte adoptará las medidas legislativas y demás que resulten necesarias para afirmar su facultad jurisdiccional respecto de cualquier conducta delictiva prevista en los artículos contenidos en la sección primera del capítulo 2 concerniente al derecho penal sustantivo que regula el presente convenio.

2.3. CAPÍTULO III – COOPERACIÓN INTERNACIONAL

Este apartado abarca las regulaciones concernientes a la cooperación internacional (artículo 23), la extradición (artículo 24) y la asistencia mutua (artículos 25 al 28) que ha de permear las relaciones entre los estados parte del convenio, para perseguir de forma idónea los delitos cibernéticos, puesto que por el carácter transfronterizo de los mismos se torna imperante contar con el apoyo de los demás estados para así poder aprehender a quien cometió tales infracciones penales.

Cabe resaltar el artículo 35 pues es este el que da mayor ilustración sobre los compromisos adquiridos para poder entablar una debida y correcta cooperación internacional, toda vez que impone a los estados parte el tener un punto localizable las 24 horas del día, los siete días de la semana, para de esta forma poder garantizar la obtención en formato electrónico de las pruebas de un delito por medio de un procedimiento acelerado, para esto han de asegurar la disponibilidad de personal formado y equipado, tal articulo reza:

"ARTICULO 35 - RED 24/7

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

A. Asesoramiento técnico;
B. Conservación de datos, de conformidad con los artículos 29 y 30;
C. Obtención de pruebas, suministro de información de carácter jurídico y localización de sospechosos.

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

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

3. Cada parte garantizara la disponibilidad de personal formado y equipado con objeto de facilitar el funcionamiento de la red."[7]

2.4. CAPÍTULO IV. – CLÁUSULAS FINALES.

Este es el último capítulo del convenio y como su nombre lo indica contiene las disposiciones finales del mismo, las cuales, en términos generales, recogen los preceptos habituales de los tratados del Consejo de Europa, tales como lo son:

Firma y entrada en vigor (Art 36) ; Adhesión al convenio (Art 37) ; Aplicación territorial (Art 38) ; Efectos del convenio(Art 39);Declaraciones(Art 40); Clausula federal (Art 41); Reservas(Art 42); Mantenimiento y retirada de las reservas (Art 43); Enmiendas (Art 44); Solución de controversias (Art 45); Consultas entre las partes (Art 46); Denuncia (Art 47); Notificación (Art 48).

ESTADOS PARTE:

El Convenio de Budapest sobre la Ciberdelincuencia ha sido ratificado por 60 estados, dentro de los cuales se encuentran lo estados parte de la Unión Europea,

[7] Convenio sobre la ciberdelincuencia, Articulo 35° - Red 24/7, Capítulo III – Cooperación Internacional. (2001), Budapest, Noviembre 23

y además de estos, el aludido convenio también ha sido ratificado por países no europeos, entre los cuales están: Estados Unidos, Canadá, Australia, Japón, Israel, República Dominicana, Chile, Argentina, Cabo Verde, Costa Rica, Filipinas, Mauricio, Marruecos, Panamá, Senegal, Sri Lanka, Tonga, Perú, Paragua, Sudáfrica y Colombia.

Colombia fue invitada por el Consejo de Europa para adherirse al convenio el 11 de septiembre de 2.013, luego de que el Gobierno Nacional adelantara las gestiones pertinentes, las cuales estaban encaminadas a contar con instrumentos jurídicos y de cooperación internacional para enfrentar la ciberdelincuencia, el estado colombiano se adhirió formalmente el 16 de marzo de 2.020, cuando depositó ante el Consejo de Europa en Estrasburgo, el instrumento de adhesión al convenio de Budapest, que es el estándar mundial en la lucha contra la ciberdelincuencia[8].

III. REGULACIÓN EN COLOMBIA.

3.1. MARCO NORMATIVO

Fue en razón al auge de la criminalidad en el ámbito informático y en conjunción a la necesidad del Estado colombiano por alcanzar una altura normativa que estuviese al nivel de los demás estados soberanos -los cuales con anterioridad ya habían tipificado las infracciones concernientes con el abuso de los sistemas informáticos y los datos personales, por medio de la adopción y seguimiento de los lineamientos contenidos dentro del *"Convenio sobre la Ciberdelincuencia de Budapest"*- que dentro del Congreso de la República surgió una iniciativa para regular tales temáticas conforme a los estándares internacionales.

PROYECTO DE LEY 042 DE 2.007.

Fue esta la primera iniciativa que surgió para regular las temáticas concernientes a la ciberdelincuencia, este proyecto de ley emerge dentro de los debates frente al tema que se llevaron a cabo en la Cámara de Representantes y cuyo ponente fue el Dr. GERMAN VARON CONTRINO.

[8] https://www.cancilleria.gov.co/newsroom/news/colombia-adhiere-convenio-budapest-ciberdelincuencia

Este proyecto de ley buscaba tanto adicionar, como modificar algunos de los tipos penales regulados dentro del Capítulo VII del Título III del Libro Segundo del Código Penal, respecto *"de la violación a la intimidad, reserva e interceptación de comunicaciones",* este proyecto de ley también velaba por endurecer las penas de ciertos delitos como lo eran el: hurto calificado (art. 240), el daño en bien ajeno (art. 265), la violación de reserva industrial o comercial (art. 308) y el espionaje (art. 463); siempre y cuando las referidas infracciones penales se cometieran a través de medios informáticos.

Para lograr ese cometido, el aludido proyecto de ley, dentro de su exposición de motivos señalaba tres modelos legislativos posibles para materializar las mencionadas adiciones y modificaciones al Código Penal, estas fueron:

I. Ley especial – que no sería integrada al Código Penal.
II. Capítulo especial – que sería incorporado al estatuto sustantivo.
III. Modificación de los tipos penales existentes.

Se optó por la modificación de los tipos penales existentes, para de esta forma garantizar la protección de los demás bienes jurídicos que también se verían afectados con estas conductas desviadas vinculadas con la ciberdelincuencia, como lo son la intimidad, la propiedad, la libre competencia y hasta la misma seguridad del estado.

Con esta modalidad (la de modificar los tipos penales existentes) se propendía por mantener las conductas existentes dentro de sus capítulos correspondientes sin alterar así los bienes jurídicos protegidos, puesto que lo que se buscaba con este proyecto de ley era agravar las conductas ya tipificadas y/o ampliar el verbo rector de los mismos, pero nunca veló por modificar a plenitud lo contenido dentro del Código Penal, a pesar de que pretendía tipificar comportamientos no contemplados en la ley penal.

La principal razón para haber decidido que se debían de modificar los tipos penales existentes, era porque a pesar de que son varias las conductas las que emplean medios informáticos para la comisión de tales infracciones penales, las mismas no

corresponden a lo que se entiende por *“delito informático”,* sino que son delitos *tradicionales* con nuevas formas de Comisión.

PROYECTO DE LEY 123 DE 2007

Posterior a lo anterior surgió una nueva iniciativa legislativa, el proyecto de ley 123 de 2.007 de la Cámara de Representantes cuyos ponentes fueron los Dres. CARLOS ARTURO PIEDRAHÍTA y LUIS HUMBERTO GÓMEZ GALLO; este proyecto de ley proponía la creación de un nuevo bien jurídico para la protección de la información, en contraposición con el proyecto de ley 042 de 2.007, el cual velaba era por la modificación de los tipos penales existentes.

Siendo así las cosas, se evidenció la necesidad de proteger tanto el patrimonio económico como los sistemas informáticos de las amenazas que representaba la ciberdelincuencia y por tanto se acumularon ambos proyectos de ley; el 042 de 2.007 en conjunto con el 123 también de 2.007.

Lo anterior fue dando surgimiento a la proposición de crear el Título VII BIS, el cual haría parte del Libro Segundo de la Parte Especial del Código Penal, este inédito conglomerado velaría por la salvaguarda de la información y de los datos, y tomaría como sustento normativo las conductas y demás lineamientos regulados dentro del Convenio sobre la ciberdelincuencia de Budapest.

El cometido de crear un nuevo título para el Código Penal colombiano, en razón al surgimiento de un inédito bien jurídico para nuestro ordenamiento, conllevó a que se separara en dos conjuntos de normas las conductas que resultarían lesivas para el emergente bien jurídico:

I. El primero sería: *“de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos”* y las conductas allí consagradas fueron: acceso abusivo a sistema informático, obstaculización ilegítima de sistema informático o red de telecomunicación, interceptación ilícita de datos informáticos o de emisiones electromagnéticas, daño informático, uso de software

malicioso *(malware),* violación de datos personales *(hacking),* suplantación de sitios web para capturar datos personales *(phishing).*

II. El segundo capítulo versaría sobre: *"de los atentados informáticos y otras infracciones"* y las conductas allí consagradas fueron: el hurto por medios informáticos y semejantes, la transferencia no consentida de activos, la falsedad informática, el espionaje informático, la violación de la reserva industrial o comercial valiéndose medios informáticos.

Los proyectos de ley referidos (042 y 123 del 2.007) fueron puestos en conjunto y así se obtuvo en un primer momento el visto bueno por parte de la Cámara de Representantes, pero su tramitación en el Senado no corrió con la misma suerte, la negatividad en tal órgano legislativo fue tal que inclusive se analizó la posibilidad de darle un archivo definitivo al proyecto de ley, toda vez que se le consideraba como algo innecesario, bajo el entendido de que ya existían tipos penales, los cuales en términos generales englobaban las conductas a reprimir por el proyecto de ley en trámite.

Una ilustración clara de este sentir es el injusto penal concerniente al hurto por medios informáticos y semejantes, ya que la ponencia en el Senado sostenía que se asimilaba al hurto agravado por el numeral 4 del artículo 240 del Código Penal[9], el cual agrava el hurto tras "*superar seguridades electrónicas u otras semejantes"* (entre otras agravantes) y que por tanto era indebido regular como nuevo algo ya existente.

Pero a pesar de lo anterior, la Comisión Primera del Senado llegó al acuerdo de no dar un archivo definitivo al emergente proyecto de ley, siempre y cuando los tipos penales que pretendían ser regulados e incorporados por este se sometieran a una serie de modificaciones.

[9] ARTICULO 240. HURTO CALIFICADO. La pena será de prisión de seis (6) a catorce (14) años, si el hurto se cometiere: 4. Con escalonamiento, o con llave sustraída o falsa, ganzúa o cualquier otro instrumento similar, o violando o superando seguridades electrónicas u otras semejantes. (Subrayas fuera del texto)

Tales modificaciones versaron en eliminar del articulado los tipos de: falsedad informática, espionaje informático y violación de reserva industrial o comercial, tras estos reparos fue aprobado el proyecto de ley por la plenaria del Senado.

Con base a lo expuesto se puede afirmar que el nuevo título – VII BIS – del Código Penal colombiano propende por regular los delitos informáticos, al igual que para proteger la información y los datos de carácter electrónico, y además de lo anterior el legislador colombiano aprovechó esta oportunidad para enfatizar en la represión del apoderamiento ilícito de los dineros pertenecientes al mercado financiero y fue así como se dio origen a la Ley 1273 DE 2.009.

LEY 1273 DE 2.009

El TITULO VII BIS, denominado *"De la Protección de la información y de los datos",* fue adicionado por el artículo 1° de la Ley 1273 del 5 de enero de 2.009; *"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.*[10]*"*

La conjunción de los proyectos de ley 042 y 123 de 2.007, conllevaron a la expedición de la referida ley, y es por medio de esta que el ordenamiento jurídico colombiano adopta los lineamientos del Convenio sobre la Ciberdelincuencia de Budapest, esto se hizo porque se consideraba de vital importancia que dentro de nuestro ordenamiento jurídico existiesen las directrices de la legislación europea frente a los delitos cibernéticos, aún cuando el Estado colombiano ni siquiera había sido invitado para adherirse al aludido convenio.

A modo de ilustración los delitos incorporados por esta ley son:

CAPÍTULO PRIMERO **DE LOS ATENTADOS CONTRA LA CONFIDENCIALIDAD, LA INTEGRIDAD Y LA DISPONIBILIDAD DE LOS DATOS Y DE LOS SISTEMAS INFORMÁTICOS**

[10] Ley 1273 de 2.009

ARTÍCULO	DELITO
269A	Acceso abusivo a un sistema informático
269B	Obstaculización ilegitima de sistema informático o red de telecomunicación
269C	Interceptación de datos informáticos
269D **269E**	Daño informático Uso de software malicioso
269F	Violación de datos personales
269G	Suplantación de sitios web para capturar datos personales
269H	Circunstancias de agravación punitiva

CAPÍTULO II **DE LOS ATENTADOS INFORMÁTICOS Y OTRAS INFRACCIONES**	
ARTICULO	**DELITO**
269I	Hurto por medios Informáticos y semejantes
269J	Transferencia no consentida de activos

Su incorporación no quedó exenta de polémicas, ya que se estaba adoptando someramente unos lineamientos jurídicos extranjeros que no contaban con el debido respaldo jurídico local, ejemplo de esto es que dentro del ordenamiento colombiano no se tenían las definiciones propias contenidas en el Convenio de Budapest, a modo de ejemplo se señaló que dentro del ordenamiento no existía definición alguna para *"sistema informático"* (entre otras tantas).

Eventos como el referido con anterioridad, entorpecieron la persecución de tales delitos por parte del ente acusador, toda vez que no había claridad respecto de las conductas a perseguir, vulnerando de esta forma el principio de la tipicidad[11] contenido en el artículo 10 del Código Penal colombiano, lo cual conllevó a que varios procesos penales abiertos en razón de estas conductas delictivas,

[11] Articulo 10 Ley 599 de 2.000 – Tipicidad; La ley penal definirá de manera inequívoca, expresa y clara las características básicas estructurales del tipo penal.

terminaban siendo archivados por parte de la Fiscalía, quien argumentaba que lo hacía porque *"no existen motivos o circunstancias fácticas que permitan su caracterización como delito"*[12] y también en muchas otras actuaciones la Fiscalía solicitaba la preclusión argumentando la "*atipicidad del hecho investigado"*[13]

Por lo anterior, la incorporación de esta ley en nuestro ordenamiento trajo consigo el emergente bien jurídico "*de la protección de la información y de los datos"* al igual que trae una serie de tipos penales para proteger al mismo, aunque lo anterior no se tradujo en condenas efectivas para los transgresores de estas disposiciones, toda vez que el ente acusador era incapaz de perseguir las mismas por las dudas que generaban los aludidos enunciados normativos.

LEY 1928 DE 2.018

Es a través de esta ley que se aprueba *"el Convenio sobre la Ciberdelincuencia"* adoptado el 23 de noviembre de 2.001 en Budapest.

Colombia fue invitada por el Consejo de Europa para adherirse al convenio sobre la Ciberdelincuencia el 11 de septiembre de 2.013 -esto es cuatro años después de la incorporación a nuestro ordenamiento jurídico de la ley 1273 de 2.009 por medio de la cual se creaba el bien jurídico *"de la protección de la información y de los datos"* con sus respectivos tipos penales- el término estipulado para formalizar la adhesión es de cinco años, por tanto el Estado colombiano tuvo hasta el año 2.018 la posibilidad de aceptar dicha invitación, y fue por medio de esta ley que se aprobó formalmente lo dicho por el aludido convenio.

3.2. CONTEXTO NACIONAL

Colombia fue el primer país en América Latina en contar con una conexión a internet de alta velocidad y con ello se tuvo como finalidad estatal el llevar esta tecnología a todos sus ciudadanos a lo largo del territorio nacional, por tanto, y desde el año

[12] Articulo 79 Ley 906 de 2.004 – Archivo de las diligencias; Cuando la fiscalía tenga conocimiento de un hecho respecto del cual constate que no existen motivos o circunstancias fácticas que permitan su caracterización como delito, o indiquen si posible existencia como tal, dispondrá el archivo de la actuación

[13] Artículo 332 Ley 906 de 2.004 – Causales: El fiscal solicitará la preclusión en los siguientes casos… #4 atipicidad del hecho investigado.

2.005, el Estado colombiano se obligó a mejorar su seguridad respecto de la información digital. En el año 2.010 se implementa en el país el *Plan vive digital*[14]*,* que conllevó a que la nación tuviera una revolución digital, donde el uso de las tecnologías de la información y comunicaciones se vuelven herramientas indispensables para el desarrollo económico y social.

Ilustración de lo anterior es que para el año 2.016 las conexiones de banda ancha en el país pasaron de 213 millones en 2.010 a 15.130 millones y que los municipios con conexión a internet ascendieron a 1075[15].

El Estado colombiano comenzó a fortalecer la seguridad interna respecto de la información digital, en la medida en que un mayor número de ciudadanos comenzaron a emplear tales tecnologías en su día a día, y por tanto se emitió el Decreto 1078[16] de 2.015 el cual obligaba a las entidades del Estado para implementar el modelo de seguridad y privacidad respecto de Tecnologías de la Información.

Con el aumento de la conectividad en el país también se incrementaron las amenazas cibernéticas, las vulnerabilidades y los incidentes digitales, perjudicando así intereses legítimos y la seguridad tanto de las personas como de las entidades públicas y privadas, toda vez que son muchas las actividades socioeconómicas que se soportan en el uso de las tecnologías de la información y comunicaciones.

NORMATIVIDAD PÚBLICA

El país venía implementando diversos instrumentos normativos, los cuales valoraban y trataban las temáticas concernientes a la seguridad de la información, y de la ciberdelincuencia.

Ejemplificación de lo anterior es la ya mencionada Ley 1273 de 2.009, que modificó el Código Penal, al adoptar los lineamientos del Convenio de Budapest, esto se hizo

[14] Es el plan de la tecnología en Colombia, busca que el país de un gran salto tecnológico mediante la masificación de internet y el desarrollo del ecosistema digital nacional
[15] Datos del Ministerio de Tecnologías de la Información y las Comunicaciones (2.016)
[16] Decreto único reglamentario del sector de tecnologías de la información y las comunicaciones.

porque se consideraba que dentro del ordenamiento interno debían existir desarrollos normativos que siguieran las directrices de la legislación europea.

Permeados con el ánimo de estimular la cooperación, colaboración y asistencia, en lo que respecta a la ciberdelincuencia, fue que Colombia se planteó la adhesión a diferentes convenios y tratados en la materia, donde resalta el Convenio de Budapest, el cual tiene por objeto materializar una política criminal común internacional y por tanto es este el estándar mundial en seguridad digital.

IMPORTANCIA DEL CONVENIO DE BUDAPEST PARA COLOMBIA

Las amenazas del ciberespacio y de las nuevas tecnologías, logran impactar de manera amplia, rápida y significativa los ámbitos públicos y privados, tanto de las personas naturales como de las personas jurídicas y por tanto tales amenazas se tornaron en un punto de común preocupación para todos los países.

Son muchas las ocasiones en las cuales los actores de las conductas punibles que afectan la ciberseguridad, se encuentran localizados en una jurisdicción distinta de donde se materializan los efectos de sus conductas, de forma tal que las pruebas de tales actos delictivos se vuelven inaccesibles a no ser que se cuente con la cooperación de las autoridades que rigen sobre esos territorios; por tanto la cooperación internacional se vuelve esencial con miras a enfrentar y prevenir los actos delictivos en materia cibernética y por tanto Colombia tenía la obligación de adherirse al Convenio sobre la Ciberdelincuencia del Consejo de Europa.

Se tornó entonces como algo imperante la debida adhesión del Estado colombiano al referido convenio; en un primer lugar por ser este el único instrumento internacional que abarca todas las áreas concernientes a la ciberdelincuencia (el derecho penal, el derecho procesal penal y la cooperación internacional), y en segundo lugar porque el convenio trata con un carácter prioritario la política penal contra la ciberdelincuencia en cada uno de los estados parte del mismo.

El Convenio de Budapest sobre la Ciberdelincuencia permite entablar lazos de cooperación internacional contra los delitos informáticos y de igual forma fortalece

tanto las leyes como las regulaciones internas ante las amenazas de la ciberdelincuencia.

En razón a la exposición que antecede es que el Gobierno Nacional, a través de la Ministra de Relaciones Exteriores, el Ministro de Justicia y del Derecho, el Ministro de Defensa Nacional y el Ministro de Tecnologías de la Información y las Comunicaciones, solicitaron al Congreso de la Republica aprobar el proyecto de Ley *"Por medio de la cual se aprueba el Convenio sobre la Ciberdelincuencia"*, adoptado el 23 de noviembre de 2.001 en Budapest.

IV. CONTROL DE CONSTITUCIONALIDAD.

4.1. SENTENCIA C-224/19

Tal como lo establece la jurisprudencia de la Corte Constitucional [17], el control que realiza esta Corporación sobre los tratados públicos y sus respectivas 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, toda vez que es enviado directamente por el Presidente de la República a la Corte Constitucional; (iii.) integral, ya que se analizan tanto los aspectos formales como materiales del tratado; (iv.) tiene fuerza de cosa juzgada; (v.) es condición indispensable para su ratificación; y (vi.) cumple una función preventiva para garantizar la supremacía de la Carta Nacional.

En atención al Convenio de Budapest, procedió la Corte Constitucional a realizar un estudio sobre si el mismo se adecuaba a la Constitución Nacional, haciendo una revisión formal y material del referido articulado internacional:

- Revisión formal: aquí se examinaron dos aspectos; el primero fue la validez de la representación del Estado colombiano en las fases de negociación, celebración y firma del convenio. La segunda, fue la observancia de las reglas del trámite legislativo.

[17] 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

- Revisión material o de fondo: consistió en confrontar las disposiciones objeto de análisis con el texto constitucional, esto se realiza con miras a determinar si el Convenio de Budapest se ajustaba o no al ordenamiento interno.

4.1.2. ANÁLISIS FORMAL

SUSCRIPCIÓN DEL ACUERDO

Se examinaron las facultades del representante del estado para negociar y adoptar el Convenio objeto de análisis, para luego incorporar el referido instrumento internacional. Siendo así las cosas, el entonces presidente de la República, Juan Manuel Santos, impartió la respectiva aprobación ejecutiva el día 8 de junio de 2.017, por medio de la cual autorizó someter a consideración del Congreso de la República el Convenio de Budapest. Se concluyó que la adopción de tal instrumento internacional satisfizo el requisito de forma respecto de la persona que fungió como representante estatal.

OBSERVANCIA DE LAS REGLAS DEL TRÁMITE LEGISLATIVO

- ASUNTO PREVIO: NECESIDAD Y REALIZACIÓN DE CONSULTA PREVIA COMO EXPRESIÓN DEL DERECHO FUNDAMENTAL A LA PARTICIPACIÓN DE LOS GRUPOS ÉTNICOS:

La sentencia C-750 de 2.008 [18] señaló que toda medida legislativa o administrativa que logré afectar de forma directa a una población étnica debe someterse a la consulta previa de los grupos étnicos, en razón al derecho fundamental que les asiste a dichas comunidades para decidir sobre sus prioridades en su desarrollo y preservación cultural.

Tras una revisión del texto del Convenio de Budapest se llega a la conclusión de que tal contiene una serie de normas homogéneas para todos los Colombianos, ya que el convenio no tiene como fin expedir una regulación específica para las comunidades étnicas; por tanto, el convenio no constituye ni tiene medidas

[18] 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

legislativas o administrativas que afecten de forma particular a las referidas comunidades y por tanto su consulta previa no se tornaba obligatoria.

- ❖ EXAMEN DEL TRÁMITE DE LA LEY 1928 DE 2.018 ANTE EL CONGRESO DE LA REPÚBLICA:

La Carta Nacional no señala un procedimiento especial para las leyes aprobatorias de tratados internacionales ni para su incorporación en la legislación interna, por tanto, a estas les corresponde el trámite estipulado para las leyes ordinarias.

- ❖ TRÁMITE ANTE EL SENADO

El proyecto de ley fue radicado en el Senado por el Gobierno Nacional el 1º de agosto de 2.017, luego de que el proyecto de ley con su respectiva exposición de motivos fuera publicado en la Gaceta del Congreso Nro 631, también del 1º de agosto de 2.017. El texto definitivo fue aprobado en 2° debate en la plenaria del Senado y fue publicado en la Gaceta del Congreso Nro 118 del 10 de abril de 2.018.

- ❖ TRÁMITE EN LA CÁMARA

Radicado el proyecto de ley de la referencia en la Cámara de Representantes, fue repartido a la Comisión Segunda Constitucional de esta corporación.

La Comisión Segunda discutió y aprobó el proyecto de ley de la referencia en la sesión realizada el 17 de mayo de 2.018, según consta en el acta Nro 26 publicada en la Gaceta del Congreso Nro 401 del 8 de junio de la misma anualidad. Según acta No 296 de la sesión del 20 de junio de 2.018, la Plenaria de la Cámara aprobó el proyecto de ley a través de votación nominal y pública, como consta en la Gaceta del Congreso Nro 912 de 2.018.

Concluye la Cámara de Representantes que, desde el punto de vista formal, la Ley 1928 de 2.018 cumplió con el procedimiento legislativo previsto en la Carta y en la Ley 5 de 1992[19].

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

Tras culminar el análisis de forma respecto al procedimiento de aprobación del proyecto de ley 1928 de 2.018, prosigue la Corte Constitucional a realizar el estudio material del Convenio de Budapest.

4.1.3. ANÁLISIS MATERIAL O DE FONDO:

En este acápite procede la Corte Constitucional a hacer un estudio sobre las disposiciones normativas contenidas en el Convenio de Budapest y a reglón seguido, sobre si tales disposiciones se ajustan a lo dicho por la Carta Nacional.

DISPOSICIONES DEL CONVENIO

- PREÁMBULO: OBJETIVO Y NECESIDAD:

El objetivo del convenio es crear una política criminal común respecto de los delitos vinculados a la ciberdelincuencia, para tal cometido se pretender proteger los intereses legítimos en la utilización y en el desarrollo de las tecnologías de la información, de forma tal que es por medio de un instrumento internacional de cooperación (como lo es el convenio) que se logra instaurar una legislación pertinente para este cometido.

- CONSTITUCIONALIDAD DE LAS NORMAS DEL CAPÍTULO I: TERMINOLOGÍA:

Aquí se establecen una serie de definiciones para efectos de comprensión del Convenio, definiciones que determinan el contenido y alcance del mismo; entiende la Corte que la referida terminología resulta necesaria para la correcta interpretación del articulado y a reglón seguido afirma que tales conceptos técnicos están en armonía con lo preceptuado por la Constitución Nacional.

- CONSTITUCIONALIDAD DE LAS NORMAS DEL CAPÍTULO II: MEDIDAS QUE DEBERÁN ADOPTARSE A NIVEL NACIONAL; SECCIÓN 1- DERECHO PENAL SUSTANTIVO.

El Convenio sobre la Ciberdelincuencia invita a la adopción de una serie de medidas legislativas que han de ser incorporadas en el derecho interno de los estados parte, esto con el fin de así poder imputar a quienes infrinjan las normativas contenidas en

este acápite, de forma tal que se garantice de esta forma la imposición de las medidas sancionatorias pertinentes, toda vez que se tipifican los delitos dentro de los ordenamientos internos.

Entiende la Corte que las disposiciones referidas en este acápite no contrarían ni desconocen los derechos constitucionales del ordenamiento jurídico colombiano, tan es así que los delitos tipificados en el Convenio se subordinan a las regulaciones del derecho interno, toda vez que el fin de las disposiciones normativas del convenio es velar por garantizar la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos.

- SECCIÓN 2- DERECHO PROCESAL PENAL

En este acápite se consagra la legislación procesal referente al Convenio, establece las facultades otorgadas a las autoridades competentes, para investigar, juzgar y condenar a quienes infrinjan las normativas contenidas en el articulado, y por tanto se garantice de esta forma la imposición de las medidas sancionatorias pertinentes.

Luego de analizar tales enunciados normativos, concluye la Corte Constitucional que: (i.) el convenio señala que sus disposiciones se aplicarán de conformidad con el derecho interno de cada estado parte, (ii.) en aras de garantizar la vigencia del ordenamiento constitucional, el Gobierno Nacional se reservará el derecho de aplicar las medidas contenidas en los artículos 20 y 21 (*obtención en tiempo real de datos sobre el tráfico e interceptación de datos sobre el contenido)* de conformidad con la normativa referida al *habeas data* y a la protección de la intimidad, esto porque tales artículos se refieren a la interceptación del contenido en tiempo real.

Con base en lo anterior, señala la Corte que las medidas de la *Sección 2- Derecho Procesal Penal* serán aplicadas: (i.) de conformidad a las limitaciones, restricciones y procedimientos establecidos en el orden interno, (ii.) con el ánimo de garantizar la vigencia del ordenamiento constitucional y por tanto el Gobierno Nacional se reservará el derecho de aplicar las medidas referidas a la “interceptación del contenido en tiempo real” (artículos 20 y 21) de conformidad con la normativa interna en materia de habeas data y protección a la intimidad.

- SECCIÓN 3 - JURISDICCIÓN

El convenio establece dentro de este epígrafe que cada estado parte deberá adoptar las medidas legislativas y demás que resulten pertinentes para imponer su autoridad y por tanto delimitando así su jurisdicción respecto de cualquier delito previsto dentro del convenio que se haya cometido dentro de su territorio o embarcación oficial.

De lo anterior entiende la Sala Plena de la Corte Constitucional que tal disposición se adecua y respeta tanto las reglas como los principios constitucionales de la nación.

- CONSTITUCIONALIDAD DE LAS NORMAS DEL CAPÍTULO III: COOPERACIÓN INTERNACIONAL.

Primeramente, se establecen los principios concernientes a la cooperación internacional, acto seguido se fijan los principios relativos a la extradición y finaliza con los procedimientos propios a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables. Lo anterior se hace bajo los términos de equidad, reciprocidad y conveniencia nacional.

Para la Sala Plena de la Corte Constitucional estas disposiciones se ajustan al marco constitucional, toda vez que están encaminadas a facilitar la cooperación efectiva entre las partes, promocionando esta forma los mecanismos propios que aseguran la implementación y promoción del convenio; lo anterior se halla en total armonía con los principios del derecho internacional aceptados por Colombia toda vez que atienden lo dicho y estipulado por nuestra Carta Política.

- CONSTITUCIONALIDAD DE LAS NORMAS DEL CAPÍTULO IV: DISPOSICIONES FINALES.

En este punto se regulan aspectos procedimentales propios de cualquier tratado internacional, mismos que de ninguna manera vulneran la Constitución Nacional.

Se introducen formas propias de los acuerdos internacionales, como lo son: 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, las reservas y el retiro de estas, las enmiendas, las soluciones de controversias, las consultas entre las partes, la denuncia y las notificaciones.

Encuentra la Corte Constitucional que estas disposiciones reflejan aspectos operativos y técnicos propios de cualquier instrumento internacional y por tanto no se vulnera la Carta Magna.

En merito de lo expuesto, concluye la Corte Constitucional que tanto el Convenio sobre la Ciberdelincuencia como su norma aprobatoria, la Ley 1928 de 2.018, son plenamente respetuosas de las disposiciones constitucionales colombianas.

V. CONCLUSIONES

Como se evidenció y se refirió a lo largo de la exposición, *El Convenio sobre la Ciberdelincuencia de Budapest,* surge por la necesidad general de tener una política criminal en común entre los diferentes países, a pesar de que esta iniciativa nace de la mano del Consejo de Europa, se tuvo la consciencia de que se estaba ante una oportunidad global para contar con un instrumento de cooperación internacional que pretende hacerle frente a las amenazas y peligros que representa el ciberespacio.

Fue por lo anterior que el Estado colombiano, inició las labores legislativas pertinentes para incorporar el Convenio de Budapest dentro de su legislación interna, a través de la ley 1273 de 2.009 con la que se creó el bien jurídico *"de la protección de la información y de los datos"*, modificando así el Código Penal.

Consecuencia de lo anterior, es que se procedió a incorporar de forma debida lo reseñado en el *Convenio de Budapest,* toda vez que a pesar de que el mismo sirvió como sustento para la promulgación de la Ley 1273 de 2.009, la misma no quedó exenta de polémica ni controversias debido a que contaba con una serie de "lagunas" y por tanto el Gobierno Nacional adelantó las gestiones pertinentes ante al Concejo de Europa para lograr la invitación y posterior adhesión al *Convenio sobre la Ciberdelincuencia*, terminando tal proceso con la promulgación de la Ley aprobatoria No 1928 de 2.018.

VI. REFERENCIAS

Normas jurídicas

Convenio sobre la Ciberdelincuencia, Budapest, Noviembre 23 de 2.001

Colombia. Constitución Política (1991)

Colombia. Congreso de la República. Ley 599 (2000). Por la cual se expide el Código Penal. Colombia. Congreso de la República. Ley 906 (2004). Por la cual se expide el Código de Procedimiento Penal.

Colombia Congreso de la Republica. Ley 1273 (2.009). 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"

Colombia. Congreso de la Republica. Ley 1928 (2.018). Por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia", adoptado el 23 de Noviembre de 2.001, en Budapest

SENTENCIAS

Corte Constitucional (2.019) Bogotá D.C. Sentencia C-224/19. Sala Plena

Tribunal Superior de Medellín (2.017). Sentencia Radicado Nro 2014-22638. Magistrado Ponente Cesar Augusto Rengifo Cuello

PÁGINAS WEB

European Committee on Crime Problems recuperado el 27 de Julio de 2.021, *https://www.coe.int/en/web/cdpc*

Library of Congress, about Kaspersen, H.W.K, recuperado el 27 de Julio de 2.021, https://id.loc.gov/authorities/names/n88071169.html

Consejo de Ministros de la Unión Europea recuperado el 27 de Julio de 2.021 https://www.uexternado.edu.co/catedra-jean-monnet/consejo-ministros-la-union-europea/

Síntesis del Consejo de Europa recuperado el 27 de Julio de 2.021 https://www.coe.int/es/web/about-us/structure

Colombia se adhiere al Convenio de Budapest contra la ciberdelincuencia recuperado el 28 de Julio de 2.021 https://www.cancilleria.gov.co/newsroom/news/colombia-adhiere-convenio-budapest-ciberdelincuencia

El Plan vive digital recuperado el 28 de Julio de 2.021 https://mintic.gov.co/portal/vivedigital/612/w3-propertyvalue-6106.html

Decreto 1078 de 2015 Sector de Tecnologías de la Información y las Comunicaciones recuperado el 29 de Julio de 2.021 https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=77888

Modelo de seguridad MinTic recuperado el 30 de Julio de 2.021 https://www.mintic.gov.co/gestion-ti/Seguridad-TI/Modelo-de-Seguridad/

Tecnologías de la información y las comunicaciones recuperado el 30 de Julio de 2.021 https://www.mintic.gov.co/portal/inicio/Glosario/T/5755:Tecnologias-de-la-Informacion-y-las-Comunicaciones-TIC