

**PREVENCIÓN Y SANCIÓN DEL DELITO INFORMÁTICO DE  
PORNOGRAFÍA INFANTIL EN COLOMBIA DE LA  
SENTENCIA T-724 DE 2003**

**JORGE OCTAVIO GARZON PINEDA**

**UNIVERSIDAD COLEGIO MAYOR DE CUNDINAMARCA  
FACULTAD DE DERECHO  
BOGOTÁ D.C.  
2022**

**PREVENCIÓN Y SANCIÓN DEL DELITO INFORMÁTICO DE  
PORNOGRAFÍA INFANTIL EN COLOMBIA SENTENCIA  
T-724 DE 2003**

**JORGE OCTAVIO GARZON PINEDA**

**TRABAJO PARA OPTAR AL TÍTULO DE ABOGADO.**

**DIRECTOR DE MONOGRAFÍA  
Dr. HERNÁN LÓPEZ LÓPEZ**

**UNIVERSIDAD COLEGIO MAYOR DE CUNDINAMARCA  
FACULTAD DE DERECHO  
BOGOTÁ D.C.  
2022**

**NOTA DE ACEPTACIÓN.**

**11 de abril de 2022.**

**Director de Monografía  
Dr. HERNÁN LÓPEZ LÓPEZ**

**Jurado 1**

**Jurado 2**

**Fecha, abril de 2022**

## AGRADECIMIENTOS Y DEDICATORIAS

*El esfuerzo y la dedicación en la carrera de Derecho, es un ejemplo y consecuencia de las personas que están a mi lado brindándome apoyo y alentando al logro de mis objetivos. El esfuerzo realizado dentro de este trabajo de investigación va principalmente dedicado a mis padres, por el apoyo a mi educación y por ser mis concejeros de vida.*

*El producto de este trabajo de investigación, obedece en gran medida a la ayuda de mis compañeros Erika Martínez, Fernando Casas, Sebastián Baquero y Sofía Cabezas, además de la colaboración del Dr. Hernán López López, con quien comparto un profundo respeto y admiración; a la Dra. Johanna Fernanda Navas y al Dr. David Muñoz, que no hay un ápice de duda que los aprecio mucho.*

*De igual manera, quiero agradecer a mis compañeros de estudio, profesores y personal educativo que fueron los que me acompañaron en cada paso que di.*

*"Nada se pierde mientras el valor permanezca." (Napoleón Bonaparte)*

**Jorge Octavio Garzón Pineda**

**Las opiniones expresadas en el presente documento son de responsabilidad exclusiva de los autores y no comprometen de ninguna forma a la Universidad Colegio Mayor de Cundinamarca a su Facultad de Derecho.**

## **RESUMEN.**

Conforme a las denominadas modalidades de delincuencia organizada transnacional, especial trascendencia adquiere la práctica de pornografía infantil habida cuenta de la vulneración sistemática y flagrante de los derechos humanos y la necesidad que le asiste a los Estados de dar una respuesta oportuna y eficaz en su detección, prevención y represión, conforme a los instrumentos regulatorios internacionales y nacionales.

Las modalidades delictivas que se desarrollan a partir del inadecuado manejo de las Tecnologías de la información y comunicación (TIC), permiten la estructuración de los delitos informáticos, escenario preferente para la configuración de la fenomenología de pornografía infantil mencionada.

En el estado actual de cosas, la criminalidad informática no cuenta con una adecuada regulación o normativa internacional, toda vez que los gobiernos y sus organismos de control presentan dificultades en la persecución y judicialización de aquellos criminales u organizaciones delictivas que se enriquecen con la comercialización y venta de la pornografía infantil en cualquiera de sus modalidades (grooming, sexting, fishing, entre otras).

En este reducto, la comunidad internacional debe aunar esfuerzos y establecer medidas más eficientes que permitan proteger a todas aquellas personas que son víctimas directas e indirectas de la pornografía infantil.

Para la sociedad colombiana el tema no es exógeno y, por el contrario, paulatinamente encuentra niveles de expansión, dificultad investigativa y por ende creciente impunidad.

El propósito de esta investigación se circunscribe a la identificación de la problemática existente y a la presentación de una alternativa de solución, acorde con las necesidades apremiantes de la sociedad colombiana.

Palabras Clave: Delitos Informáticos, ciberdelincuentes, Internet, Delincuencia Transnacional, pornografía infantil, comunidad internacional, Grooming, Hacking,

### **ABSTRACT**

In accordance with the so-called modalities of transnational organized crime, special significance of child pornography given the systematic and flagrant violation of human rights and the need for states to provide a timely and effective response in their detection, prevention, and repression, in accordance with international regulatory instruments.

The criminal practices that develop from the inadequate handling of Information and Communication Technologies (ICTs), allow the structuring of computer crimes, the preferred setting for the configuration of the aforementioned practice of child pornography.

In the current state of affairs, computer crime does not have adequate international regulations or standards, since States and control bodies present difficulties in the prosecution and prosecution of those criminals or criminal organizations that are enriched by the commercialization and sale of child pornography in any of its forms (grooming, sexting, fishing, among others).

In this stronghold, the international community must join forces and establish better measures to protect all those people who are direct and indirect victims of child pornography.

For Colombian society, the issue is not exogenous and, on the contrary, it gradually finds levels of expansion, investigative difficulty, and therefore impunity.

Key Words: Computer Crimes, Circumferential, Internet, Transnational Crime, child pornography, international community, Grooming, Hacking.



## TABLA DE CONTENIDO

<b>1.</b>	<b>INTRODUCCIÓN</b>	<b>11</b>
<b>2.</b>	<b>UBICACIÓN DEL PROBLEMA</b>	<b>14</b>
2.1.	Descripción del problema	14
2.2.	Formulación del problema	15
2.3.	Justificación	15
2.4.	Objetivos	19
2.4.1.	Objetivo general	19
2.4.2.	Objetivos específicos	19
<b>3.</b>	<b>MARCO METODOLOGICO.</b>	<b>20</b>
<b>4.</b>	<b>MARCO DE REFERENCIA.</b>	<b>24</b>
4.1.	Marco histórico	24
4.2.	Marco jurídico	34
4.3.	Marco institucional	40
4.4.	Marco teórico conceptual	54
<b>5.</b>	<b>CAPITULOS</b>	<b>65</b>
5.1.	Capítulo uno: generalidades de la delincuencia organizada transnacional y delito informático de pornografía infantil.	65
5.1.1.	Generalidades de la Delincuencia Organizada Transnacional ¡Error! Marcador no definido.	
5.1.2.	Pornografía Infantil ¡Error! Marcador no definido.	
5.2.	Capítulo dos: regulación del delito informático de pornografía infantil	77
5.2.1.	Instrumentos de derecho internacional	77
5.2.2.	Delito Informático.	82
5.2.3.	instrumentos de derecho interno	84
5.2.4.	Regulación de la Pornografía Infantil.	89
5.3.	Capítulo tres: modalidades de pornografía infantil en Colombia: la informática como medio de masificación delincriminal.	95
5.3.1.	Caracterización de la pornografía infantil en Colombia.	95
5.3.2.	Estadísticas de la Pornografía infantil en Colombia.	97
5.4.	Capítulo cuatro: Alternativa regulatoria de prevención contra la proliferación de la pornografía infantil	102
<b>6.</b>	<b>CONCLUSIONES</b>	<b>106</b>
<b>7.</b>	<b>REFERENCIAS</b>	<b>107</b>
7.1.	Referencias Documentales	107
7.2.	Documentos Electrónicos.	111
7.3.	Referencias Jurisprudenciales	112

**TABLA DE GRÁFICOS**

Gráfico 1. Material ESNNA	95
Gráfico 2. Explotación Sexual Comercial de Niños, Niñas y Adolescentes	96
Gráfico 3. Estadística de denuncia por delitos.	97

## 1. INTRODUCCIÓN

La criminalidad informática constituye un aspecto fundamental para la concepción post moderna del Derecho, en consideración a que la denominada www (world wide web) la red informática mundial de internet ha sido empleada como el medio y el escenario propicio para la comisión de conductas delictuales de diversa índole, destacándose el progresivo e incontrolado aumento del delito de pornografía infantil.

Con el paso del tiempo los medios tecnológicos han tenido un vertiginoso avance, incluyendo mayores grados de dependencia por parte del ser humano frente a las tecnologías de la información y comunicación (TIC), ya que los modos y medios de producción han adaptado la prestación de servicios, el consumo de bienes y la oferta de productos a esta nueva dinámica globalizada.

El constante avance e innovación que presentan las TIC, encuentran aplicación ilegal en las prácticas de delincuencia tanto organizada como individual, a través de la realización de los denominados delitos informáticos.

A manera de ejemplo, podemos referir el delito de pornografía infantil, cuando el cibercriminal utiliza indebidamente los medios tecnológicos para obtener imágenes explícitas de contenido erótico, teniendo como víctima a menores de edad, acude a la estrategia del anonimato y/o adoptar falsas identidades.

En segundo término, El victimario informático puede estar en cualquier parte del mundo sin ser detectado, esto es posible en razón a que

existen programas que ocultan las direcciones IP (Protocolo de internet)<sup>1</sup>, programas como los denominados: Tor, Onion Browser, y Tor Browser entre otros, permitiendo navegar y compartir la información de contenido íntimo de manera más segura para sus propósitos criminales, facilitando la comercialización ante la gigantesca red de pedófilos o pederastas como principales consumidores de dicho contenido erótico.

En tercera instancia, podría estar tomando información de una red de tráfico de contenido sexual de menores de edad para comercializar su producto en diferentes Estados, como consecuencia de la facilidad en la transmisión de datos. En efecto práctico, una red de tráfico online que se ubique en Europa como expendedor de pornografía infantil tendría la posibilidad de venta simultánea a consumidores de otros continentes.

Los Ciberdelincuentes en la internet tienen un amplio espacio de comunicación y transmisión de datos ilícitos, representando uno de los inconvenientes más complejos para la mayoría de los Estados tratándose de la persecución y judicialización de los ciberdelincuentes.

No obstante, las medidas adoptadas por los organismos de control como la Organización para la Cooperación y el Desarrollo Económicos- OCDE; la Organización de Naciones Unidas- ONU; la Unión Europea, el Consejo de Europa, la ECPAT<sup>2</sup> y la CEOP<sup>3</sup> -Destacando esta última organización internacional especializada en la persecución del delito informático de pornografía infantil- han originado debates y transfigurado los mecanismos en

---

<sup>1</sup> Identificador de dirección única que permite reconocer el dispositivo en internet o en una red local.

<sup>2</sup> ECPAT es el acrónimo de End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes (Acabar con la Prostitución Infantil, la Pornografía Infantil y el Tráfico de Niños con fines Sexuales).

<sup>3</sup> Centro de Protección Contra la Explotación de Menores en la Red.

los Estados en defensa de los derechos de los niños y la respectiva punición del delito de pornografía infantil.

Estas instituciones han determinado que en materia de Derecho Internacional es bastante complicado judicializar y capturar a la delincuencia transnacional, debido a que la ilicitud de sus actos se enfrenta a tres elementales factores para determinar la competencia y principios como del juez natural, expresado en los paradigmas de extraterritorialidad<sup>4</sup>, territorialidad objetiva y subjetiva<sup>5</sup>, así como nacionalidad activa y pasiva<sup>6</sup>.

El delito informático, tiene carácter transnacional merced a la posibilidad de distanciamiento espacial (por las redes informáticas internacionales), entre el lugar donde el autor realiza la acción delictiva y el lugar donde se producirán los efectos o consecuencias negativas, aspecto que supera el ámbito de aplicación de la normatividad nacional.

---

<sup>4</sup> En el principio de la extraterritorialidad, el Estado extiende la vigencia de su ley penal a delitos cometidos fuera de su territorio (C-1189-00 Corte Constitucional de Colombia)

<sup>5</sup> En la territorialidad subjetiva, el Estado puede establecer y aplicar normas sobre actos que se iniciaron en su territorio, pero culminaron en el de otro Estado y en la territorialidad objetiva cada Estado puede aplicar sus normas a actos que se iniciaron por fuera de su territorio, pero culminaron o tienen efectos sustanciales y directos dentro de él (Sentencia C-527/03 Corte Constitucional de Colombia).

<sup>6</sup> La nacionalidad activa, habilita al Estado para dictar normas de conducta de obligatoria observancia para sus nacionales, así estén en el exterior, y la nacionalidad pasiva, según el cual el Estado puede ejercer jurisdicción sobre personas, actos o cosas que lesionen los intereses de uno de sus nacionales en territorio extranjero.

## **2. UBICACIÓN DEL PROBLEMA**

### **2.1. Descripción del problema**

La expansión y fortalecimiento de la delincuencia organizada transnacional, indica que, para el caso colombiano, se registran niveles acelerados de crecimiento e impunidad, deslegitimación institucional y ausencia de políticas públicas en materia de prevención, educación y formación sexual, fenomenologías de alto impacto social y evidentes repercusiones jurídicas que determinan, el campo de interés de la presente investigación, representado en el delito de pornografía infantil.

En el ámbito jurídico nacional e internacional los instrumentos regulatorios encaminados a la prevención, judicialización y sanción del delito de pornografía infantil, no responden de manera eficaz a la manera exponencial y consolidada como las organizaciones criminales de carácter transnacional, obtienen beneficios económicos incalculables e instrumentalizan a los menores de edad, quienes en virtud a su notoria condición de indefensión e inferioridad como víctimas, son usados para vejámenes como la explotación y/o abuso sexual y a través de los mismos menores la atracción de nuevas víctimas infantiles.

En este reducto, la comunidad nacional e internacional, adquiere el deber histórico de establecer medidas más eficaces que garanticen la protección de todas aquellas personas víctimas de la pornografía infantil. En el caso de Colombia el mencionado delito, posee un alto nivel de comercialización e impunidad.

## **2.2. Formulación del problema**

¿Cuales mecanismos jurídicos de orden nacional e internacional, debieran implementarse para la prevención, investigación y represión eficaz del delito informático de pornografía infantil en Colombia?

## **2.3. Justificación**

La influencia negativa de las tecnologías de la información y las telecomunicaciones en las actuales sociedades post modernas, infortunadamente han auspiciado la sofisticación de la delincuencia organizada transnacional, ya que los constantes flujos de información, el procesamiento y transferencia automática y desmedida de datos a nivel mundial, representa un inminente riesgo para las generaciones presentes y futuras.

El proceso de globalización ha permitido la consolidación de formas explícitas de delincuencia organizada transnacional, proyectándose en el infinito ciber espacio, condición que ubica a la pornografía infantil como una de las actividades criminales más rentables en la actualidad, compartiendo dicho estatus con otras actividades ilícitas como el tráfico de armas, narcotráfico, trata de personas entre otras.

La expansión de la criminalidad informática, encuentra parcialmente explicación en la aparición de la comunicación de la red entre personas y el mercado de módems, terminales económicos, elementos tecnológicos de relativo fácil acceso, así como por la inversión de cuantiosos recursos económicos, humanos, logísticos e infraestructura puesta al servicio de los denominados ciberdelincuentes para materializar sus conductas criminales.

Los delitos informáticos de mayor operatividad en la actualidad están representados en las practicas del phishing, scamming, grooming, la estafa informática, cyberbullyng entre otros, explicados en buena parte por el proceso transicional entre los grupos poblacionales de nativos digitales y migrantes tecnológicos.

La comunidad internacional ha venido estableciendo medidas de diversa índole tendientes a contrarrestar las principales prácticas de delitos informáticos, que desde la década de los años 60 irrumpieron en las relaciones sociales, permitiendo la intromisión ilegal en información personal, confidencial y amparada por reserva legal como la bancaria y financiera.

La razón misma de que las personas y los menores de edad, se convirtieron en víctimas, es que el hombre se está adaptando cada vez más las TIC, y para los cibercriminales adoptan con el paso del tiempo más herramientas tecnológicas para poder beneficiarse en la comercialización de material de pornografía infantil y cometer otras modalidades de delitos informáticos.

Los cibernautas cada vez son más susceptibles a ser víctimas de los criminales cibernéticos, ya que el ser humano desarrolla procesos de dependencia tecnológica, tanto en su espacio laboral como personal incrementando potencialmente el riesgo de ser víctima de la criminalidad informática.

Las autoridades tienen un complejo problema para controlar la consumación de delitos informáticos, toda vez que la captura y judicialización de los infractores plantea un verdadero reto para los organismos y entes de control.



En la década de los años 90 aparece el delito de pornografía infantil en la internet, comercializándose imágenes de contenido sexual de menores de edad, resulta que el delito informático de pornografía infantil posee las mismas complicaciones que los demás delitos informáticos, debido a la información cibernética y los programas que utilizan los Ciberdelincuentes y/o pederastas que comercializan en el mercado negro de internet ese material de contenido erótico.

El mencionado delito lo define, el docente López el cual asevera la definición más acertada de pornografía infantil: “La pornografía infantil expresa [...] Integra aquella conducta explícita desarrollada en la que participa un menor de edad un claro ejemplo podría ser el de un adulto que graba a un menor mientras es penetrado por un tercero.” (López, 2015, p. 115)

Actualmente, no existe una adecuada prevención en la política criminal global que permita que las personas y menores de edad, manejen adecuadamente la red, y no sean fácilmente engañados por delincuentes que elaboran trampas cibernéticas principalmente para contactar a niños y jóvenes, que son los principales sujetos pasivos de las acciones punibles ya mencionadas.

Las Naciones, han elaborado una serie de instrumentos jurídicos alrededor de estos delitos en sus territorios y, hasta hace pocos años con la expansión de la red, han logrado observar que estos tienen un problema de carácter transnacional y que tienen unas innumerables conexiones con la delincuencia organizada transnacional, toda vez que, con la globalización se dio alcance no sólo a desarrollos comerciales y tecnológicos sino también a la ampliación y consolidación del crimen.

Es necesario que se fortalezcan los instrumentos de derecho nacional e internacional que regulen la actividad de la delincuencia organizada transnacional en los delitos informáticos de carácter sexuales ya mencionados.

El delito informático de pornografía infantil ha generado una considerable cantidad de capital en el mercado negro a las organizaciones criminales organizadas, la cual ha acelerado la oferta y la demanda en la comercialización del material ilícito y erógeno.

En consecuencia, resulta estratégico que los Estados como sujetos de derecho internacional público continúen adquiriendo compromisos frente a la comunidad internacional que permitan una correcta persecución, judicialización, así como, una política criminal de prevención educativa. De esta forma Colombia se ha vinculado a una serie de compromisos internacionales con el fin solucionar este problema criminal informático.

Colombia, infortunadamente se enfrenta al delito de pornografía infantil, que desde los años 90 ha tenido un progresivo aumento. El Estado colombiano hasta hace más de 10 años ha comenzado realmente una política criminal en contra de los ciberdelincuentes, pero no ha sido suficiente para contrarrestar este flagelo, siendo necesario en la actualidad adoptar una política criminal mucho más estricta para contrarrestar la pornografía infantil.

Así pues, esta investigación tendrá un enfoque cualitativo que se centra principalmente en el análisis de textos que permitan esclarecer las principales características de la pornografía infantil del contexto colombiano y el alcance internacional; analizando comparativamente ejemplos de diferentes países que permitan dilucidar las posibles alternativas de solución desde el ámbito jurídico con base en una política criminal.

## **2.4. Objetivos**

### **2.4.1. Objetivo general**

Analizar las estrategias de intervención del derecho internacional y nacional para la pornografía infantil como modalidad del delito informático en Colombia.

### **2.4.2. Objetivos específicos**

- Identificar la problemática de la delincuencia organizada transnacional entorno al delito informático de pornografía infantil en Colombia.
- Determinar las modalidades constitutivas de la pornografía infantil que se adelanta a través del uso de TICS en Colombia.
- Analizar los instrumentos internacionales y nacionales que regulan el delito informático de pornografía infantil.
- Proponer una alternativa regulatoria de prevención al delito informático de pornografía infantil en Colombia.

### 3. MARCO METODOLOGICO.

La presente investigación socio-jurídica es de tipo teórica, y se ubica dentro de las ciencias sociales, la metodología es de carácter cualitativo, debido a que se usan datos sobre estimaciones de expertos jurídicos, doctrina, jurisprudencia etc., se realiza la recolección de datos a partir de categorías u proporciones teóricas que enriquecen el cuerpo de información para desarrollar mejor la investigación se puede revalidar en el texto del investigador Sabino cuando afirma que: *“El enriquecimiento de los datos obtenidos y que permite reunir un cuerpo de información variado y completo, muy importante para los estudios de tipo cualitativo.”* (Sabino, 1992, p.17)

La monografía jurídica principalmente es de carácter exploratorio, con un enfoque en el análisis documental, en consecuencia, a la proposición teórica jurídica -decidirse de una vez por todas a conocer la realidad social tomando como referente las condiciones empíricas concretas – cuantificable y no cuantificable de vida de las poblaciones estudiadas.” (Bonilla y Rodríguez, 2005, p. 58)

En el trabajo académico se construyó un conocimiento científico que orienta a la elaboración de una estructura analítica y delimitante que parte desde la investigación en la cual con la información recolectada se conceptualizo con un estudio descriptivo y analítico, conforme a la necesidad de establecer las causalidades y consecuencias de los delitos informáticos, en consecuencia, existe una relación intrínseca de los mencionados estudios que requiere la investigación:

[...]Por tanto, la principal característica de los estudios descriptivos es que se limitan simplemente a dibujar el fenómeno estudiado, sin pretender establecer ninguna relación causal en el tiempo con ningún

otro fenómeno, para lo que necesitaríamos recurrir a un estudio analítico. [...] Los estudios Analíticos se caracterizan porque pretenden “descubrir” una hipotética relación entre algún factor de riesgo y un determinado efecto, es decir, pretenden establecer una relación causal” (Veiga de Cabo, J., & Zimmermann Verdejo, M., 2008, p.3-4)

La presente monografía tiene un enfoque de hermenéutica dialéctica debido a que se basa en la relación dialéctica entre la comprensión, la explicación y la interpretación, si bien ellas se dan en unidad dialéctica donde la interpretación es la síntesis entre la comprensión y la explicación; en el proceso de investigación científica, se produce un movimiento en el cual estos procesos van adquiriendo mayor relevancia en el desarrollo del propio proceso investigativo, así se indica conforme a los lineamientos de los docentes Ruedas, Ríos y Nieves:

[...] La investigación suele surgir a partir de un examen de la bibliografía y la identificación de un problema. Así pues, los pasos más relevantes en toda investigación hermenéutica son: a) la identificación de algún problema; b) la etapa empírica que incluye la identificación de textos relevantes y su correspondiente validación; c) la etapa interpretativa en la que se buscan las pautas en los textos. Éstos se explican para generar una interpretación, la relación de la nueva con las existentes [...] (Ruedas Marrero, M., Ríos Cabrera, M. M., & Nieves, F, 2009, p.115)

Así en las primeras etapas del trabajo monográfico, la comprensión del marco teórico, la elaboración del diagnóstico y el estudio, adquieren un mayor significado en la comprensión del objeto de la investigación que va transitando a la explicación del problema transnacional y nacional del delito informático, desde una conciencia del hombre esencialmente histórico-causal,

como podemos observar en el marco histórico que explicará el origen del delito informático de pornografía infantil.

De esta forma el enfoque que tendrá este estudio será cualitativo, en la medida en que se analizarán de forma rigurosa las categorías conceptuales anteriormente planteadas para responder al problema de investigación formulado, en palabras del metodólogo Hernández Sampieri: “Describir, comprender e interpretar los fenómenos, a través de las percepciones y significados producidos por las experiencias de los participantes.” (Sampieri, 2014, p.11).

Es así, que se propende con la investigación socio-jurídica exploratoria, la necesidad de investigar los fenómenos y la aplicación del pensamiento dialectico, a través de un análisis documental y académico, que permita de la formulación de una conjetura que se compruebe y/o intente en el ordenamiento jurídico:

[...] hay dedicación comprometida con el fenómeno bajo escrutinio e investigación sistemática, crítica, abierta y autorreflexiva. La investigación explicativa, conducida de esta forma, se transforma en un instrumento de ampliación de conocimiento, de concientización, y de expansión conceptual e intelectual. (Reiter. 2015, p. 164)

La técnica a utilizar en la presente investigación consiste en un análisis documental de las categorías conceptuales que se estudian, encontrando su desarrollo en diversos textos académicos, doctrina, jurisprudencia etc., además de esta manera se obtienen los datos fundamentales para justificar la investigación de orientación socio-jurídica. De conformidad con los textos académicos nos permite ayudar a entender el

problema jurídico central, en palabras del profesor Sampieri: “Le permiten al investigador para conocer y/o analizar las circunstancias de un ambiente, así como las experiencias y/o situaciones que acontecen.” (Sampieri, 2014, p.415)

El presente marco pretende identificar y ofrecer un enfoque e instrumento metodológico para la elaboración de la presente investigación desde niveles de comprensión y explicación que desarrollen el análisis del objeto de investigación y su aplicación en el mundo jurídico colombiano.

## **4. MARCO DE REFERENCIA.**

### **4.1. Marco histórico**

Los ordenadores tecnológicos han permeado todos los ámbitos de las relaciones socioeconómicas, así como las esferas de la actividad del hombre, individual o socialmente consideradas, en virtud a los grados de interdependencia y necesidad informativa.

Sectores como la administración pública, el bancario, la actividad aseguradora, los medios de transporte con especial énfasis en el transporte aéreo y terrestre, la educación, la actividad bursátil, entre otras, dependen en buena parte de las computadoras, como consecuencia de que estos aparatos electrónicos y eléctricos han invadido todo tipo de negocios y empresas, además de una apreciable cantidad de hogares y oficinas, por la miniaturización de los computers chips de la informática y telemática.

Este acelerado proceso tecnológico, infortunadamente ha elevado la delincuencia relacionada con los sistemas de procesamiento y transferencia automática de datos en conjunto con las TIC, afectando la sociedad globalizada en virtud a su carácter transnacional, en razón a que el uso indebido del ordenador y los desarrollos científicos, han permitido el posicionamiento de la ciberdelincuencia y el incremento en la comisión de dichos delitos.

Los delitos informáticos tienen origen prácticamente en la década de los años 80 y 90, ya que la comunidad internacional identificó el comienzo de la cibercriminalidad, a partir de la elaboración de una estratégica tipología de virus, razón por la cual resulta pertinente una precisión conceptual acerca de su definición. En este sentido, la Real Academia de la Lengua Española lo define de la siguiente manera: "Programa introducido subrepticamente en la



memoria de un ordenador que, al activarse, destruye total o parcialmente la información almacenada". (Real Academia Española, 2022)

Los primeros ataques a los sistemas informáticos de los Gobiernos, fueron a través de virus direccionados con finalidades específicas tales como la información reservada y de seguridad nacional, secretos industriales y comerciales entre otros.

El pionero de dicha práctica en contra del Gobierno de Estados Unidos, fue el hacker Robert Tappan Morris quien fue conocido por crear el Gusano Morris en 1988, considerado como el primer gusano de ordenador de la era de Internet. Se estima que en ese momento el tamaño de Internet era de unos 60.000 ordenadores, y el gusano afectó cerca de 6 000 sistemas de ordenadores en los Estados Unidos (incluyendo el centro de investigación de la NASA) y dejó casi inútiles algunos de ellos. Dicho en palabras de los investigadores:

En realidad, nunca se sabrá exactamente cuántos computadores resultaron infectadas porque con el hecho de reiniciar el equipo se eliminaban todos los datos del gusano (y se contenía la infección) así que los afectados son solo un número estimado aproximado. (Manuel Y Concheiro, 2010 P. 6).

El programa intentaba averiguar las contraseñas de otras computadoras usando una rutina de búsqueda que permutaba los nombres de usuarios conocidos, una lista de las contraseñas más comunes y también búsqueda al azar. Descubrieron que no todas las computadoras eran afectadas, sino que solo se propagó en las computadoras VAX de DEC (Digital Equipment Corp) y las fabricadas por Sun Microsystems, que empleaban Unix.

En el año de 1989, aparecería un virus más peligroso que sería el virus Dark Avenger, también conocido como "vengador de la oscuridad", que se propago en Europa y Estados Unidos, ejecutando acciones perjudiciales, el profesor ruso Bontchev (1991) en que su naturaleza altamente contagiosa, ya que, sí el virus estaba activo en la memoria, al abrir o simplemente su apertura o copia era suficiente para infectar. Adicionalmente, el virus destruyó datos, al sobrescribir un sector aleatorio del disco cada 16 ejecuciones de un programa infectado, corrompiendo progresivamente los archivos y directorios del disco.

En 1990, Mark Washburn crea "1260", el primer virus polimórfico, que muta en cada infección, este virus se explica en la siguiente cita:

"Un virus de la familia de camaleón que apareció en 1990, fue desarrollado por Mark Washburn. La regla principal es la de modificar el aspecto del código constantemente de una copia a otra. Debe llevarse a cabo de tal forma que no haya cadena común permanente entre las variantes de un virus para que el motor del escáner del antivirus no lo detecte [...]" (Carrasco de la Fuente, R., Gumiel Erena, S., & Vizcaíno González, A. 2013, p.23)

Específicamente el virus mencionado lo explica y define el Centro de Seguridad Ayudaley de la siguiente manera:

El malware polimórfico es un tipo de malware que cambia constantemente sus características identificables para evadir la detección. Muchas de las formas comunes de malware pueden ser polimórficas, incluidos virus, gusanos, bots, troyanos o registradores de pulsaciones de teclas. Las técnicas polimórficas implican características

identificables que cambian con frecuencia, como nombres y tipos de archivos o claves de cifrado, para que el malware sea irreconocible para muchas técnicas de detección.

El polimorfismo se utiliza para evadir la detección de coincidencia de patrones en la que se basan las soluciones de seguridad como el software antivirus. Si bien ciertas características del malware polimórfico cambian, su propósito funcional sigue siendo el mismo. (Centro de Seguridad Ayudaley, 2021)

Para 1991, aparece el conocido virus Michelangelo sobre el cual se crea una gran alarma sobre sus daños y amplia propagación, el virus Michelangelo debe su nombre a que se activó el día seis (06) de marzo de cada año, fecha que coincide con el cumpleaños del artista italiano Miguel Ángel (06 marzo del año del año 1475).

El virus fue diseñado para infectar "Sistema Operativo de Disco" en la fecha específica del cumpleaños del artista italiano Michelangelo, como todos los virus del sector de arranque, operaba a nivel de BIOS. Cada año, el virus permaneció inactivo hasta el 06 de marzo, el cumpleaños del artista renacentista, el virus consistía en la destrucción de toda la información que poseía el usuario en su respectivo computador.

De hecho, destruye toda la información contenida en la pista 0, más concretamente los primeros 17 sectores de las cuatro primeras caras en los 250 primeros cilindros del disco infectado. Esto supone una pérdida de la información contenida en 8 MB, aproximadamente.

En síntesis, los virus más nocivos durante el siglo XX merced al daño que ocasionaron, llevaron a que la Organización de Cooperación Económica (OCDE) realizará en el año de 1986 la siguiente definición, como lo afirma la licenciada mexicana Lourdes Delgado: “Cualquier conducta ilegal, no ética o no autorizada que involucra el procesamiento automatizado de datos y/o la transmisión de datos” (Delgado, 2010, p.2)

Con el avance de la tecnología comienzan los Estados, a plantearse la penalización de los llamados “delitos informáticos”, la Organización de Cooperación y Desarrollo Económico (OCDE) fue la primera entidad que contribuyo a combatir la ciberdelincuencia con un informe donde diferentes representantes oficiales afirmarían que existen en el sistema jurídico una serie de falencias entorno a la punibilidad en relación con estas conductas criminales.

En el año de 1986, la OCDE expidió en Paris un manual llamado “Computer Related Crimes: Analysis of legal policy”, señalando la existencia de cinco formas principales de “criminalidad informática” las cuales son a.) La falsificación informática; b.) El fraude informático; c.) El sabotaje informático; d.) La copia ilegal de programas informáticos, y e.) El acceso ilegal a sistemas informáticos.

A continuación, se presentan las definiciones de las formas principales de criminalidad informática, haciendo la salvedad de que éstas han sido replanteadas de acuerdo a los nuevos retos que afronta la comunidad.

La falsificación informática es definida como:

(...) Introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la

intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente. (Políticas sobre Criminalidad Informática y Legislación en Centro América, 2012)

El fraude informático es definido como:

(...) los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante: a. la introducción, alteración, borrado o supresión de datos informáticos; b. cualquier interferencia en el funcionamiento de un sistema informático, con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona. (Políticas sobre Criminalidad Informática y Legislación en Centro América, 2012)

El sabotaje Informático guarda cierta similitud con el fraude informático, sin embargo, lo diferencia el modo de operación, así pues, la definición es:

Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son: Bombas lógicas (logic bombs), es una especie de bomba de tiempo que debe producir daños posteriormente. Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro; Gusanos. Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse; Virus informáticos y malware; Ciberterrorismo. Terrorismo informático es el acto de hacer algo para desestabilizar un

país o aplicar presión a un gobierno, utilizando métodos clasificados dentro los tipos de delitos informáticos, especialmente los de los de tipo de Sabotaje, sin que esto pueda limitar el uso de otro tipo de delitos informáticos, además lanzar un ataque de terrorismo informático requiere de muchos menos recursos humanos y financiamiento económico que un ataque terrorista común; Ataques de denegación de servicio: Estos ataques se basan en utilizar la mayor cantidad posible de recursos del sistema objetivo, de manera que nadie más pueda usarlos, perjudicando así seriamente la actuación del sistema, especialmente si debe dar servicio a mucho usuarios. (Foro de Profesionales Latinoamericanos de Seguridad, 2012)

Por último, la Ley 1273 de 2009<sup>7</sup>, (Colombiana) define el acceso ilegal a sistemas informáticos en los siguientes términos:

Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo.

La Organización de Naciones Unidas en el año de 1994 realizó el correspondiente manual sobre la prevención y control del delito informático, en el cual clasifica cinco modalidades frecuentes de delito informático así: El fraude por manipulación informática; la falsificación informática; los daños o modificaciones de datos informáticos o programas, o sabotaje informático; el acceso no autorizado a sistemas informáticos y de servicio, y la reproducción no autorizada de programas informáticos legalmente protegidos.

---

<sup>7</sup> Normatividad sobre delitos informáticos. Art. 269A.

La ONU a raíz de este manual, determino que es necesario que la mayoría de bloques continentales realicen una política criminal adecuada, como estrategia frente al problema criminal de los ciberdelincuentes, estableciendo en el mismo documento que los Estados creen una serie de mecanismos de control social y de poder, teniendo como objetivos prevenir y disminuir la criminalidad; fortalecer los aparatos investigativos; otorgar las garantías procesales y sustanciales a los intervinientes en la investigación, respetando así las libertades y garantías del ciudadano.

La ONU principalmente desarrollo este manual, debido a que, con el avance de la tecnología, los Ciberdelincuentes se encontraban en un potencial aumento y organización, porque en la red se estaban (y aún sigue sucediendo) conformando grupos de delincuencia transnacional organizada, que cometían diferentes tipos de delitos informáticos.

La Unión Europea en el año de 1998 le encargo la dirección de un estudio de los delitos informáticos llamado COMCRIME-STUDY al reconocido penalista y docente Alemán Ulrich Sieber, este informe consiste en un análisis de las seis áreas de la delincuencia informática, en términos del docente Del Canto asevera lo siguiente:

“(...) informe establece seis áreas de delincuencia informática: la protección de la intimidad la legislación penal económica, la protección de la propiedad intelectual, los comportamientos ilegales perjudiciales, la legislación procesal penal y la regulación sobre seguridad. En la red de los delitos informáticos agrupa cinco tipos generales: el acceso informático ilegal o hacking, el espionaje informático, la piratería de software y otras formas similares, el sabotaje y la extorsión informática y el fraude informático. (Del Canto, 2002, p.324)

El Consejo de Europa es una de las organizaciones que se ha preocupado más por la problemática de los delitos informáticos a nivel internacional, dado que los pronunciamientos que realiza este organismo internacional en cuanto a la prevención y persecución por medio de sus Consejos de Ministros, emiten una serie de recomendaciones con destino a todos los Gobiernos que pertenecen al Consejo de Europa, destacándose las recomendaciones No. (81)12, N.R (81)20 y No. R (89) 9. (Europa, Consejo de Europa, 2004)

Juristas expertos en el tema de delitos informáticos en los años de 1985 y 1989, realizaron para el Consejo de Europa un informe sobre la delincuencia transnacional, postulando la necesidad en diseñar una política criminal basada en la prevención de las formas de ciberdelincuencia y cibercriminalidad, así como en la identificación y solución al problema que se suscita en la aplicación de la ley penal en los ámbitos territorial o espacial; personal y temporal.

El estudio presentando por los expertos, también plantea como objetivo la creación de figuras jurídicas para que los Estados miembros del Consejo Europeo, lograrán legislar y enfrentarse a unos pocos delitos informáticos. En este sentido, Suarez señala lo siguiente:

“(...) El Comité de expertos también fijó una lista opcional que aludía a figuras delictivas cuya creación en las legislaciones nacional resultaba conveniente pero no imprescindible para lograr el objetivo, entre las que se encontraban la alteración de datos o programas informáticos, el espionaje informático y el uso no autorizado de ordenadores o programas protegidos. [...] Los estudios realizados por aquel comité de expertos se concretaron en la emisión de la recomendación No.R. 89(9)



Del 13 de septiembre de 1989, en cuyo texto el Consejo de ministros del Consejo de Europa adoptó la clasificación antes mencionada. (...) (Suarez, 2009, p. 70)

La primera entidad en catalogar la pornografía infantil como delito informático, fue el Consejo de Europa en la Convención que se realizó en Budapest el 23 de noviembre de 2001. Este Convenio es el primer tratado internacional sobre delitos cometidos a través de Internet y otras redes informáticas, que versa en particular sobre las infracciones a derechos de autor; fraude informático; pornografía infantil; los delitos de odio y violaciones de seguridad de red. También contiene una serie de competencias y procedimientos, tales como la búsqueda de las redes informáticas y la interceptación legal.

La circulación de comercio de la Pornografía Infantil no comienza en los años 2000, esta tiene su origen en los años 90, lo aseveran así los docentes Sergio y Omar, en la siguiente cita señalan que:

[...] El origen del fenómeno podría rastrearse hasta la génesis misma de Internet -mediados del siglo pasado, verificando un crecimiento acelerado desde la década del noventa por la conjunción de una serie de factores. Entre estos últimos, se destacan la propagación exponencial de las computadoras personales y otros dispositivos (*smartphones, tablets, smartwatches, smartglasses*),” (Delgado, Franca, 2014, p. 3)

Conforme a lo anterior es necesario señalar que el mencionado delito informático, ha estado siempre presente con el auge de la red de internet y, es un negocio del mercado negro que adquiere unos gananciales significativos.

Desde los años 90 se ha presentado un aumento considerable de la comercialización de contenido erótico. En los años 2003 y 2007 tuvo un auge considerable en el mundo, así se señala en el informe de la señora Najat Maalla M'jid que es una política y diplomática marroquí que sirve como la Representante Especial del Secretario General de las Naciones Unidas para Violencia contra Niños, citando en su informe lo siguiente:

(...) Además de su creciente número, las imágenes de niños explotados sexualmente son cada vez más espeluznantes. Las imágenes son cada vez más violentas y los niños que aparecen en ellas, cada vez más pequeños. El número de imágenes de "explotación grave de niños" se cuadruplicó entre 2003 y 2007; el 47% de los sitios analizados contienen brutales imágenes de abusos sexuales a niños. (ONU, 2009, P. 9)

#### **4.2. Marco jurídico**

El Convenio Budapest, es el primer tratado internacional que buscó hacer frente a los delitos informáticos, el 23 de noviembre de 2001 fue suscrito en la ciudad de Budapest y entró en vigor el 01 de julio de 2004. A partir del 28 de octubre de 2010, 30 Estados firmaron, ratificaron y se adhirieron a la Convención, entre los cuales se incluye Colombia, toda vez que de acuerdo al ordenamiento jurídico colombiano a través del Congreso de la República promulga la Ley 1928 de 2018, disposición por medio de la cual se adopta como legislación interna el Convenio de Budapest, siendo sometido a control de constitucionalidad por parte de la honorable Corte Constitucional, disposiciones declaradas exequibles a través de la Sentencia C-224/19.

Este convenio en especial enmarca una serie de delitos informáticos que son los siguientes: Derechos de autor; fraude informático; pornografía

infantil; los delitos de odio y violaciones de seguridad de red de los sistemas informáticos. Estos delitos, se comprenden en el amparo de los derechos de la creación propia, la exposición íntima, pertenencia a un grupo social frente a la difusión de esos contenidos delictivos en medios como literatura, imágenes, videos, dibujos, entre otros.

El principal objetivo consiste en aplicar una política criminal penal encaminada a la protección de la sociedad contra el cibercrimen, mediante la admisión de una legislación adecuada y el fomento de la cooperación internacional para enfrentarse a la delincuencia informática transnacional.

El instrumento internacional aludido, consagra aspectos de derecho procesal penal identificando el problema transnacional que tienen la mayoría de delitos informáticos; la preservación expeditiva de los datos almacenados; la preservación expeditiva y divulgación parcial de los datos de tráfico; la orden de producción, búsqueda e incautación de datos informáticos; la recolección en tiempo real del tráfico de datos y la interceptación de datos de contenido, en procura de materializar una verdadera persecución de la delincuencia transnacional.

El Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual (2007), constituye un tratado multilateral mediante el cual los Estados acuerdan criminalizar ciertas formas de abuso sexual contra los niños, constituyéndose en el primer tratado internacional que se ocupa del abuso sexual infantil.

El prenombrado instrumento internacional, establece una adecuada persecución de carácter penal para aquellas personas que cometan delitos de carácter sexual en contra de un menor de edad, también este convenio se

centra en la protección de los niños, así lo afirma el Consejo de Europa en su convenio:

“(...) La protección del menor es el núcleo esencial de este convenio, que se centra principalmente en el respeto de los derechos del menor, asegurando su bienestar, teniendo en cuenta sus opiniones, necesidades e inquietudes, y actuando en todo momento a favor del interés superior del menor.” (Consejo de Europa, 2010, p.2)

El instrumento regulatorio, consagra un conjunto de medidas dentro de las cuales se destacan las siguientes:

1. Medidas preventivas encaminadas a seleccionar, reclutar y formar a las personas que trabajan en contacto con niños. Garantizar que los menores son conscientes de los riesgos de explotación y abuso sexual, así como de los medios para protegerse.
2. Garantizar medidas de intervención controladas regularmente, dirigidas tanto a delincuentes sexuales como a potenciales delincuentes y encaminadas a prevenir los delitos sexuales contra menores.
3. Medidas de protección que establezcan programas de apoyo a las víctimas y a sus familias. Poner en marcha una asistencia terapéutica y atención psicológica de urgencia. Fomentar la denuncia cuando se tengan sospechas de la existencia de un caso de explotación o abuso sexual. Crear líneas de asistencia telefónica y por Internet para prestar asesoramiento.

4. Medidas de derecho penal para garantizar que determinadas conductas sean tipificadas como delitos, tales como realizar actividades sexuales con niños por debajo de la edad legal para realizarlas; tipificar como delitos conductas que se sirven de las nuevas tecnologías, en particular Internet, para agredir sexualmente a los menores, como acontece con el 'Grooming' o ciber-acoso infantil (proposiciones a menores con fines sexuales).

5. Reunir y almacenar los datos sobre delincuentes condenados por delitos sexuales contra niños. Procedimientos de investigación y judiciales adecuados a los menores, garantizando la adecuada protección de los niños víctimas durante los procedimientos, y procurar que no se agrave la experiencia traumática.

6. Proteger la intimidad, identidad e imagen de las víctimas. Establecer medidas adaptadas a las necesidades de las víctimas, respetando los derechos de los niños y de sus familias. Limitar al máximo el número de entrevistas con los menores, asegurando que éstas se realicen en entornos tranquilizadores, con profesionales formados a tal fin.

7. Crear un mecanismo de seguimiento específico para garantizar la aplicación del Convenio, asegurando, el cumplimiento de sus disposiciones por parte de los Estados para lograr su eficacia a largo plazo. Con ello se pretende asegurar que el cumplimiento del convenio por parte de los Estados, y su eficacia a largo plazo. (Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual, 2007)

La ONU a través de la UNICEF realizó el protocolo facultativo sobre la venta de niños, la prostitución y pornografía infantil, fundamentado en la Convención de Derechos de los Niños de 1989 y aprobada con la Ley 12 de 1991.

El protocolo señala una política criminal en contra de cualquier persona que tenga relación con la serie de delitos en contra de los niños, y es el caso de la pornografía infantil y la prostitución, de manera muy pedagógica, la UNICEF identifica en su articulado que conductas son catalogadas como delitos sexuales y que se encuentran encaminados en afectar a los menores de edad en su bien jurídico tutelado por el Estado, denominado libertad, integridad y formación sexual.

La UNICEF quiere que los Estados ratifiquen este protocolo, ya que según quieren confirmar la prevención establecida en el Congreso Mundial contra la Explotación Sexual Comercial de los Niños, que se celebró en Estocolmo del 27 al 31 de agosto de 1996.

El Código Penal Colombiano (ley 599 del año 2000) en su artículo 218 señala el delito de pornografía infantil, toda vez que este delito se clasifica en un tipo de conducta instantánea y de tipo mono-ofensivo, que consiste en toda aquella representación, de manera gráfica o visual, en la que se muestren conductas de contenido sexual, incluida la exhibición de genitales, por parte de menores de dieciocho años.

La conducta se constituye con un verbo determinador compuesto alternativo. El cual es fotografiar; filmar; grabar; producir; divulgar; ofrecer; vender; comprar; poseer; portar; almacenar; transmitir o exhibir el objeto material de la infracción.

Los delitos referentes al derecho de autor en Colombia recaen sobre la literatura, en la ley 23 de 1982 (Colombia) sobre de derechos de autor nos establece lo siguiente:

Los derechos de autor recaen sobre las obras científicas literarias y artísticas las cuales se comprenden todas las creaciones del espíritu en el campo científico, literario y artístico, cualquiera que sea el modo o forma de expresión y cualquiera que sea su destinación. Tales como: los libros, folletos y otros escritos; las conferencias, alocuciones, sermones y otras obras de la misma naturaleza; las obras dramáticas o dramático-musicales; las obras coreográficas y las pantomimas; las composiciones musicales con letra o sin ella; las obras cinematográficas, a las cuales se asimilan las obras expresadas por procedimiento análogo a la cinematografía, inclusive los videogramas; las obras de dibujo, pintura, arquitectura, escultura, grabado, litografía; las obras fotográficas o las cuales se asimilan las expresadas por procedimiento análogo a la fotografía; las obras de arte aplicadas; las ilustraciones, mapas, planos croquis y obras plásticas relativas a la geografía, a la topografía, a la arquitectura o a las ciencias y, en fin, toda producción del dominio científico, literario o artístico que pueda reproducirse, o definirse por cualquier forma de impresión o de reproducción, por fonografía, radiotelefonía o cualquier otro medio conocido o por conocer.

Por último, en Colombia se han sancionado leyes referentes a la lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes tales son las leyes Ley 679 de 2001, Ley 1336 DE 2009 y la reciente la Ley 2197 de 2022. De las cuales se hará un recorrido más profundo a lo largo de la investigación.

### 4.3. Marco institucional

La Organización para la Cooperación y el Desarrollo Económicos (OCDE) fundada en el año de 1961 agrupa a 35 países miembros y su misión específica, consiste en promover políticas pública y privadas que promuevan el desarrollo social y económico, especialmente en los sectores poblacionales más desprotegidos.

La OCDE ofrece diferentes foros donde los Gobiernos puedan trabajar conjuntamente para compartir y formular alternativas de solución frente a los problemas comunes. Esta entidad internacional trabaja para identificar las causas que conducen a las transformaciones económicas, sociales y ambientales, con base en la medición de la productividad y los flujos globales del comercio e inversión.

Así mismo, analiza y compara datos que permitan realizar pronósticos de tendencias, fijando estándares internacionales dentro de un amplio rango de temas de políticas públicas.

En el caso de los delitos informáticos fue la primera entidad internacional que estableció medidas para combatir la delincuencia informática, hacia el año 1986, con la realización de un encuentro en la ciudad de Paris que arrojó la expedición de un documento que refleja los inconvenientes que presenta varios países frente a los delitos informáticos, y complementariamente plantea una serie de propuestas de solución frente a los ciberdelincuentes, así lo revalida Suarez:

(...) En dicho estudio de 1986 se concluyó que existían importantes lagunas de punibilidad en las regulaciones penales de tales conductas,



vigentes en algunos países analizados, además de notables divergencias normativas de regulación entre las soluciones dadas en las legislaciones nacionales. Por tal razón se hicieron recomendaciones en pro de una armonización legislativa en materia de “criminalidad informática. (...) (Suarez, 2009, p. 66)

La Organización de las Naciones Unidas (ONU), es la mayor organización internacional existente y se define como una asociación de gobiernos global que facilita la cooperación en asuntos como el Derecho internacional, la paz y seguridad internacional, el desarrollo económico y social, los asuntos humanitarios y los derechos humanos.

La ONU fue fundada el 24 de octubre de 1945 en la ciudad estadounidense de San Francisco, por 51 países, al finalizar la Segunda Guerra Mundial, con la firma de la Carta de las Naciones Unidas.

Dicho estamento internacional expidió para el año de 1994, un documento denominado Manual sobre la prevención y control del delito informático, cuyo eje temático se focaliza en la delincuencia de carácter transnacional en el entendido que constituye uno de los principales problemas para la comunidad internacional, ya que con los avances de la tecnología y los medios informáticos están siendo empleados para fines delictivos con afectación tanto a personas naturales como jurídicas de Derecho Público y Privado, generando transgresión a los bienes jurídicamente tutelados por el Estado.

El manual de la ONU tiene un fin principal y es identificar exactamente que es el delito informático y que tipos de procedimientos jurídicos pueden sancionarlo, Suarez lo ratifica:

“(...) El mencionado Manual concluye que como la criminalidad informática es un problema internacional, es necesario sumar esfuerzos para definir el delito informático y armonizar los procedimientos procesales con el fin de sancionarlo, esto a su vez aumenta la vulnerabilidad de estas redes y crea oportunidades para su mal uso en una base transnacional. [...] la expansión de comercio e intercambio internacional promueve una necesidad concomitante de leyes que salvaguarden los intereses económicos adecuadamente. (Suarez, 2009, p. 67)

A nivel de la Unión Europea, existe el Consejo de Europa cuya naturaleza jurídica es la de una organización internacional y ámbito regional, destinado a promover, mediante la cooperación de los Estados de Europa, la configuración de un espacio político y jurídico común en el continente, sustentado sobre los valores de la democracia, los derechos humanos, el Imperio de la ley y la integración económica.

Constituido por el Tratado de Londres el 5 de mayo de 1949, el Consejo de Europa es la más antigua de las organizaciones que persiguen los ideales de la integración Europea, y es así mismo la única que integra en su seno a la mayoría de Estados de Europa.

El Consejo de Europa es una de las organizaciones que se ha preocupado más por la problemática de los delitos informáticos a nivel internacional, a partir de la conformación de un Comité integrado por los juristas más representativos en materia de Derecho Penal Internacional, realizando el Convenio de Budapest en el año 2001.

Juristas expertos en el tema de delitos informáticos en los años de 1985 y 1989 se encontraban preparando para el Consejo de Europa el Convenio de

Budapest, instrumento que versa sobre la delincuencia transnacional, la cual se tendría que enfrentar a una política criminal fundamentada en la prevención del delito y la identificación de la aplicación de la ley penal en los delitos informáticos.

Los expertos se plantearon un objetivo muy importante que fue opcional y era la creación de figuras jurídicas para que los Estados miembros del Consejo de Europa, lograrán legislar y enfrentarse a unos pocos delitos informáticos de ahí Suarez:

El comité de expertos también fijó una lista opcional que aludía a figuras delictivas cuya creación en las legislaciones nacional resultaba conveniente pero no imprescindible para lograr el objetivo, entre las que se encontraban la alteración de datos o programas informáticos, el espionaje informático y el uso no autorizado de ordenadores o programas protegidos. [...] Los estudios realizados por aquel comité de expertos se concretaron en la emisión de la recomendación No.R. 89(9) Del 13 de septiembre de 1989 [...] El Consejo de Europa habría de encontrar el origen de la emisión de la segunda recomendación referida los problemas relativos a la ley procesal vinculados a la tecnología de la información (Recomendación NO.R (95) 113 de 11 de septiembre de 1995) y de la denominada Convención sobre Cyber-crime adoptada por la asamblea de dicho organismo en Budapest.” (Suarez, 2009. p. 70)

La ECPAT es el acrónimo de *End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes*.<sup>8</sup>, la ECPAT es una red de organizaciones e individuos que conjuntamente laboran para eliminar la explotación comercial sexual de niños, niñas y adolescentes

---

<sup>8</sup> (Acabar con la Prostitución Infantil, la Pornografía Infantil y el Tráfico de Niños con fines Sexuales).

(ESCNNA). En la actualidad ECPAT cuenta con afiliados y grupos nacionales en más de 70 países que llevan a cabo varios programas en contra de la ESCNNA.

Los fines de esta organización son los siguientes: enfocar los esfuerzos para promover la conciencia acerca de los distintos tipos de ESCNNA; abocarse al diseño de políticas con autoridades nacionales e internacionales; proporcionar servicios de atención y protección para las víctimas de la explotación sexual; y, llevar a cabo programas para concientizar y sensibilizar a niños y comunidades vulnerables.

La ECPAT International funciona como una organización que busca alentar a la comunidad mundial para garantizar que los niños del mundo puedan disfrutar de sus derechos fundamentales, libres de todo tipo de explotación comercial sexual.

El CEOP es un Centro de protección contra la explotación de menores en la red, es originario de Inglaterra, pero trabaja en conjunto con el FBI, y desempeña las mismas funciones que la ECPAT, diferenciándose en el hecho de que esta organización trabaja en conjunto con el FBI de USA.

El Comando de Explotación Infantil y Protección en Línea , o el Comando CEOP , es un comando de la Agencia Nacional de Crimen del Reino Unido (NCA), y tiene la tarea de trabajar a nivel nacional e internacional para poner en línea a delincuentes sexuales infantiles , incluidos los involucrados en la producción , distribución y visualización de material de abuso infantil.

En Colombia, la Fiscalía General de la Nación se creó tras la promulgación de la Constitución Política de Colombia de 1991 en sus Artículos

249 y 250 y, asume las funciones de la Dirección Nacional de Instrucción Criminal (entidad extinta) y las planteadas en los Artículos 250 y 251:

ARTÍCULO 250. La Fiscalía General de la Nación está obligada a adelantar el ejercicio de la acción penal y realizar la investigación de los hechos que revistan las características de un delito que lleguen a su conocimiento por medio de denuncia, petición especial, querrela o de oficio, siempre y cuando medien suficientes motivos y circunstancias fácticas que indiquen la posible existencia del mismo. No podrá, en consecuencia, suspender, interrumpir, ni renunciar a la persecución penal, salvo en los casos que establezca la ley para la aplicación del principio de oportunidad regulado dentro del marco de la política criminal del Estado, el cual estará sometido al control de legalidad por parte del juez que ejerza las funciones de control de garantías. Se exceptúan los delitos cometidos por Miembros de la Fuerza Pública en servicio activo y en relación con el mismo servicio.

En ejercicio de sus funciones la Fiscalía General de la Nación, deberá:

Solicitar al juez que ejerza las funciones de control de garantías las medidas necesarias que aseguren la comparecencia de los imputados al proceso penal, la conservación de la prueba y la protección de la comunidad, en especial, de las víctimas.

El juez que ejerza las funciones de control de garantías, no podrá ser, en ningún caso, el juez de conocimiento, en aquellos asuntos en que haya ejercido esta función.

La ley podrá facultar a la Fiscalía General de la Nación para realizar excepcionalmente capturas; igualmente, la ley fijará los límites y eventos en que proceda la captura. En estos casos el juez que cumpla la función de control de garantías lo realizará a más tardar dentro de las treinta y seis (36) horas siguientes.

Adelantar registros, allanamientos, incautaciones e interceptaciones de comunicaciones. En estos eventos el juez que ejerza las funciones de control de garantías efectuará el control posterior respectivo, a más tardar dentro de las treinta y seis (36) horas siguientes.

Asegurar los elementos materiales probatorios, garantizando la cadena de custodia mientras se ejerce su contradicción. En caso de requerirse medidas adicionales que impliquen afectación de derechos fundamentales, deberá obtenerse la respectiva autorización por parte del juez que ejerza las funciones de control de garantías para poder proceder a ello.

Presentar escrito de acusación ante el juez de conocimiento, con el fin de dar inicio a un juicio público, oral, con intermediación de las pruebas, contradictorio, concentrado y con todas las garantías. Solicitar ante el juez de conocimiento la preclusión de las investigaciones cuando según lo dispuesto en la ley no hubiere mérito para acusar.

Solicitar ante el juez de conocimiento las medidas judiciales necesarias para la asistencia a las víctimas, lo mismo que disponer el restablecimiento del derecho y la reparación integral a los afectados con el delito.

Velar por la protección de las víctimas, los jurados, los testigos y demás intervinientes en el proceso penal, la ley fijará los términos en que podrán intervenir las víctimas en el proceso penal y los mecanismos de justicia restaurativa.

Dirigir y coordinar las funciones de policía Judicial que en forma permanente cumple la Policía Nacional y los demás organismos que señale la ley.

Cumplir las demás funciones que establezca la ley.

El Fiscal General y sus delegados tienen competencia en todo el territorio nacional.

En el evento de presentarse escrito de acusación, el Fiscal General o sus delegados deberán suministrar, por conducto del juez de conocimiento, todos los elementos probatorios e informaciones de que tenga noticia incluidos los que le sean favorables al procesado.

PARÁGRAFO. La Procuraduría General de la Nación continuará cumpliendo en el nuevo sistema de indagación, investigación y juzgamiento penal, las funciones contempladas en el artículo 277 de la Constitución Nacional.

PARÁGRAFO 2o. Atendiendo la naturaleza del bien jurídico o la menor lesividad de la conducta punible, el legislador podrá asignarle el ejercicio de la acción penal a la víctima o a otras autoridades distintas a la Fiscalía General de la Nación. En todo caso, la Fiscalía General de la Nación podrá actuar en forma preferente.

ARTÍCULO 251. Son funciones especiales del Fiscal General de la Nación:

Investigar y acusar, si hubiere lugar, directamente o por conducto del Vicefiscal General de la Nación o de sus delegados de la unidad de fiscalías ante la Corte Suprema de Justicia, a los altos servidores que gocen de fuero Constitucional, con las excepciones previstas en la Constitución.

Nombrar y remover, de conformidad con la ley, a los servidores bajo su dependencia.

Asumir directamente las investigaciones y procesos, cualquiera que sea el estado en que se encuentren, lo mismo que asignar y desplazar libremente a sus servidores en las investigaciones y procesos. Igualmente, en virtud de los principios de unidad de gestión y de jerarquía, determinar el criterio y la posición que la Fiscalía deba asumir, sin perjuicio de la autonomía de los fiscales delegados en los términos y condiciones fijados por la ley.

Participar en el diseño de la política del Estado en materia criminal y presentar proyectos de ley al respecto.

Otorgar, atribuciones transitorias a entes públicos que puedan cumplir funciones de Policía Judicial, bajo la responsabilidad y dependencia funcional de la Fiscalía General de la Nación.

Suministrar al Gobierno información sobre las investigaciones que se estén adelantando, cuando sea necesaria para la preservación del orden público. (Constitución Política de Colombia, 1991)



La Fiscalía General de la Nación en el asunto que nos compete en esta investigación, dispone de dos direcciones para la investigación y judicialización. La primera es Dirección Especializada Contra las Violaciones a los Derechos Humanos, para la persecución penal de las conductas atentatorias contra las garantías inherentes al ser humano. La Dirección Especializada contra los Delitos Informáticos fue creada mediante la Ley 2197 de 2022. art 68, cuya función es “liderar la investigación y judicialización de los delitos informáticos y las demás conductas delictivas conexas o relacionadas”.

Las funciones de las Direcciones especializadas comprenden de manera general en lo siguiente:

ARTÍCULO 20. FUNCIONES DE LAS DIRECCIONES ESPECIALIZADAS. (Modificado por los artículos 41 y 42 del Decreto Ley 898 de 2017) Las Direcciones Especializadas cumplirán las siguientes funciones generales:

1. Dirigir, coordinar y adelantar las investigaciones y acusaciones que le sean asignadas por recomendación del respectivo comité de priorización o directamente por el Fiscal General de la Nación, según los lineamientos de priorización y la construcción de contextos, cuando haya lugar.

2. Organizar y adelantar comités técnico-jurídicos de revisión de las situaciones y los casos para la ejecución de acciones en el desarrollo efectivo y eficiente de las investigaciones penales de su competencia. Si el fiscal del caso se aparta de la decisión del Comité deberá motivar su posición, la cual será estudiada nuevamente por este. En todo caso, en virtud de los principios de unidad de gestión y de jerarquía, prevalecerá el criterio y la posición de la Fiscalía señalada por

el Comité, en aplicación del numeral 3 del artículo 251 de la Constitución.

3. Implementar y aplicar las políticas públicas y directivas del Fiscal General de la Nación en el desarrollo de las funciones que cumple la Dirección Especializada.

4. Identificar y delimitar situaciones y casos susceptibles de ser priorizados y presentarlos a la Delegada Correspondiente.

5. Ejecutar los planes de priorización aprobados por el Comité Nacional de Priorización de Situaciones y Casos en lo de su competencia.

6. Suministrar al Delegado correspondiente la información de las investigaciones y acusaciones adelantadas por su dependencia, debidamente consolidada y clasificada.

7. Asesorar a las dependencias de la Fiscalía General de la Nación en los temas especializados de su competencia.

8. Mantener actualizada la información que se registre en los sistemas de información de la entidad, en los temas de su competencia.

9. Dar cumplimiento a las estrategias y mecanismos dados por la Delegada correspondiente para que el desarrollo de las funciones de la Dependencia se adelante de manera coordinada y articulada.

10. Elaborar e implementar los planes operativos anuales en el ámbito de su competencia, de acuerdo con la metodología diseñada por la Dirección de Planeación y Desarrollo

11. Aplicar las directrices y lineamientos del Sistema de Gestión Integral de la Fiscalía General de la Nación.

12. Las demás que le sean asignadas por la ley, o delegadas por el Fiscal o Vicefiscal General de la Nación.

13. Dirigir, coordinar y controlar la investigación y judicialización de las diversas formas de delincuencia, bien sea a nivel local, regional, nacional o transnacional incluidas las nuevas formas de criminalidad emergentes en el posconflicto. (Adicionado por el artículo 43 del Decreto Ley 898 de 2017)

14. Planear, ejecutar y controlar las funciones de policía judicial a cargo de la Dirección Especializada en el ámbito de su competencia. (Adicionado por el artículo 43 del Decreto Ley 898 de 2017)

15. Asesorar y apoyar a las dependencias de la Fiscalía General de la Nación en materia de investigación criminal y en la administración de información técnica y judicial que se requiera para la investigación penal, en los asuntos de su competencia. (Adicionado por el artículo 43 del Decreto Ley 898 de 2017)

16. Hacer análisis criminal, en el ámbito de su competencia, para apoyar el cumplimiento de las funciones de la Fiscalía General de la Nación. (Adicionado por el artículo 43 del Decreto Ley 898 de 2017)

17. Crear y coordinar grupos especializados de investigación en el ámbito de su competencia que respondan a las líneas de investigación a su cargo, bajo los lineamientos del Fiscal General de la Nación. (Adicionado por el artículo 43 del Decreto Ley 898 de 2017)

18. Apoyar, en el marco de sus competencias las actuaciones que adelanten las dependencias de la Fiscalía General de la Nación en el ejercicio de sus funciones, cuando estas lo requieran. (Adicionado por el artículo 43 del Decreto Ley 898 de 2017)

19. Mantener actualizada la información en el Registro Único de Asuntos de Policía Judicial de la Fiscalía General de la Nación, en los temas de su competencia. (Adicionado por el artículo 43 del Decreto Ley 898 de 2017)

20. Adelantar el intercambio de información entre los distintos organismos de investigación, de seguridad e inteligencia a nivel nacional e internacional y entre las distintas entidades públicas y privadas, para la programación y el desarrollo de operaciones contra la delincuencia, bajo las directrices del Vicefiscal General de la Nación. (Adicionado por el artículo 43 del Decreto Ley 898 de 2017)

21. Implementar en el desarrollo de sus competencias las políticas de aseguramiento y cadena de custodia de los elementos materiales probatorios y evidencia física. (Adicionado por el artículo 43 del Decreto Ley 898 de 2017)

22. Dirigir, coordinar y controlar en el desarrollo de las funciones que cumplen los servidores y las dependencias o grupos a su cargo, la incorporación y aplicación de políticas públicas, estrategias,

metodologías, protocolos de investigación que adopte el Fiscal General de la Nación. (Adicionado por el artículo 43 del Decreto Ley 898 de 2017)

23. Mantener canales de comunicación y coordinación con la Dirección Nacional del Cuerpo Técnico de Investigación (CTI) y con las dependencias de la entidad, en especial con las que cumplan funciones de policías judiciales o relacionadas con esta. (Adicionado por el artículo 43 del Decreto Ley 898 de 2017)

24. Dirigir, coordinar y adelantar las investigaciones y actuaciones. en materia de finanzas criminales que le sean asignadas por recomendación del respectivo comité de priorización o directamente por el Fiscal General de la Nación, según los lineamientos de priorización y la construcción de contextos, cuando haya lugar. (Adicionado por el artículo 43 del Decreto Ley 898 de 2017). (Estructura de la Fiscalía General de la Nación, 2018)

Otra institución Colombiana que hace frente al delito de pornografía Infantil es la Policía Nacional de Colombia. Su creación data el 5 de noviembre de 1891 con el Decreto 1000 sancionado por el Gobierno Nacional. Su misión es la siguiente:

El fin primordial de la Policía Nacional es el mantenimiento de la convivencia como condición necesaria, para el ejercicio de los derechos y libertades públicas y para asegurar que los habitantes de Colombia convivan en paz fundamentada en el código de ética policial. (Policía Nacional de Colombia, 2022).

Las funciones y deberes de la Policía Nacional de Colombia están contenidas en el Decreto 4222 del 23 de noviembre de 2006 “Por el cual se modifica parcialmente la estructura del Ministerio de Defensa Nacional.”, ley 1712 del 06 de marzo de 2014, artículo 9, literal “a”, corresponde entre otras, la obligación de publicar sus “deberes” los cuales se encuentran taxativamente descritos en la constitución, respectivamente.

Dentro de la policía Nacional existe un cuerpo especializado a la Policía de Infancia y Adolescencia cuyo fin es garantizar la Protección Integral de los niños, niñas y adolescentes en el marco de las competencias y funciones que le asigna la ley. Este cuerpo está compuesto por oficiales, suboficiales, Nivel Ejecutivo y Agentes, todos capacitados en Derechos Humanos, Código de la Infancia<sup>9</sup> y la Adolescencia, normas nacionales e internacionales y procedimientos de atención.

#### **4.4. Marco teórico conceptual**

Una de las definiciones más claras de delitos informáticos la realizó el fiscal Napoleón Botache, cuando establece una definición fundamentada en la ley 1273 de 2009 que guarda similitud con las definiciones de la OCDE y la ONU:

“Los delitos informáticos son aquellas conductas punibles que atacan bienes informáticos en sí mismos, y que tiene como objeto material la calidad, pureza, idoneidad y corrección de los datos e información, los componentes lógicos, transmisión o almacenamiento, ejemplo: causar

---

<sup>9</sup> Ley 1098 del 08 noviembre de 2006

daño a software mediante la introducción de un virus, o acceder sin la autorización debida a una pc.” (Napoleón, 2011, p. 127)

Los delitos informáticos son aquellas actividades ilícitas que se cometen mediante el uso de computadoras, sistemas informáticos u otros dispositivos de comunicación (la informática es el medio o instrumento para realizar un delito); o tienen por objeto causar daños, provocar pérdidas o impedir el uso de sistemas informáticos (Paloma Parra, 2012).<sup>10</sup>

Hay que identificar el inconveniente que presentan los delitos informáticos para descubrir el sujeto activo que comete la acción punible, uno de los principales problemas que tienen las autoridades es que en esta clase de actividades ilícitas existen una serie de dificultades para averiguar y encontrar materiales probatorios que puedan en un proceso penal, probar la comisión de un acción punible, porque existe el anonimato de las IPS<sup>11</sup> de cualquier elemento tecnológico con acceso a internet, la desaparición de un registro de envió de información que puede hacer el usuario en cualquier momento, con diferentes programas permitiendo afirmar que su IP se encuentra en cualquier parte del mundo.<sup>12</sup>

La comunidad que comete los delitos informáticos son los ciberdelincuentes, delincuencia informática, hackers etc., el autor Suarez Sánchez realizo la siguiente definición de las características de la delincuencia informática:

---

<sup>10</sup> Delitos informáticos (en el ciber espacio),

<sup>11</sup> Una dirección IP es un número que identifica, de manera lógica y jerárquica, a una Interfaz en red (elemento de comunicación/conexión) de un dispositivo (computadora, tableta, portátil, smartphone) que utilice el protocolo IP (Internet Protocol), que corresponde al nivel de red del modelo TCP/IP.

<sup>12</sup> La Estafa Informática, Suarez Sánchez, 2009.

“Se caracteriza la denominada delincuencia informática por la dificultad para su persecución en relación con la delincuencia tradicional o clásica en razón de la rapidez de su comisión, la distancia que puede haber entre el lugar de la realización de la acción ilícita y el de la producción del resultado, la dificultad para descubrir a los autores y la facilidad para borrar las huellas, por la posibilidad de alternar programas y datos sin dejar rastro, y la facilidad para asegurar su impunidad, pues la complejidad técnica de la materia reduce su conocimiento a un círculo limitado de expertos.” (Suarez, 2009, p.34)

Tras identificar en que consiste el delito informático en nociones resumidas, es necesario explicar de que trata el delito informático de Grooming. “Grooming” es un término de la lengua inglesa que significa “Acicalar” se utiliza para hacer referencia a todas las conductas o acciones que realiza un adulto para ganarse la confianza de un menor de edad, con el objetivo de obtener beneficios sexuales.

El sujeto activo de la acción punible del Grooming, se gana la confianza del menor de edad en el internet, a través de conversaciones por chats virtuales, redes sociales, o videojuegos online, propiciando la confianza del menor y formando una especie de amistad, conociendo los gustos, intereses y actividades favoritas de la víctima.

El adulto acude a dicha maniobra fraudulenta, con el objetivo obtener beneficios sexuales, tales como fotografías y videos del menor de edad de contenido sexual, e inclusive, incurrir en la conducta punible de secuestro simple empleado como medio para lograr cometer delitos sexuales.



En este sentido, la definición del docente H. López es la más adecuada para definir el significado del delito sexual de pornografía infantil, se define de la siguiente manera:

“Pornografía Infantil expresa: Comprende el núcleo de figuras estudiadas y tipificadas en la mayoría de ordenamientos jurídicos, en tanto integra aquella conducta sexual explícita desarrollada o en la que participa un menor de edad o incapaz, quedando sujeta a filmación o exhibición. Un claro ejemplo podría ser un adulto que graba a un menor mientras es penetrado por un tercero.” (López, 2015, p.115)

El Grooming tiene una conexión explícita con la pornografía infantil y los delitos sexuales, estos delitos cuando son cometidos vulneran el bien jurídico tutelado tienen una configuración de carácter tripartito llamado: Libertad, formación e integridad sexual.

Estos bienes jurídicos tutelados mencionados tienen una serie de elementos que son necesarios ingresar a analizar como lo son la libertad sexual y el pudor sexual, pero antes de explicar estos dos elementos es ineludible que debo acotar en que consiste los delitos sexuales, Los delitos sexuales se referencian como atentados contra la libertad, integridad y formación sexual, sin el consentimiento del titular del derecho, estos son divulgados a través de tecnologías de la información y las comunicación de esta manera según el ordenamiento jurídico penal surgen tipos penales.<sup>13</sup>

Consideramos necesario explicar el significado de libertad sexual, debido a que es un derecho que implica determinaciones que toma el ser humano en su manera de actuar sexualmente, toda vez que la libertad sexual

---

<sup>13</sup> Delitos Contra Generaciones Futuras y Derechos Fundamentales de Cuarta Generación en el Derecho Penal Internacional, Hernán López López, 2015.

es una facultad y derecho de elegir, rechazar, aceptar y auto determinar el propio comportamiento sexual, con necesaria sujeción a los conceptos éticos de la comunidad y al respeto a los derechos ajenos correlativos.<sup>14</sup>

La ley debe proteger en forma directa la determinación sexual de todo ser humano, la cual no puede ser violentada (acceso y actos sexuales violentos), ni anulada o viciada (acto sexual o acceso carnal con persona en incapacidad de resistir).<sup>15</sup>

El pudor sexual significa el recato y la vergüenza. Es un valor innato, que hace orientar el comportamiento sexual de toda persona, según principios de delicadeza y respeto por el propio cuerpo y sus órganos sexuales.

El pudor es un movimiento natural que hace que se rechace lo obsceno con sentimiento de repugnancia y se proteja la propia intimidad corporal. Es reflejo de la sublimidad de las formas e instintos sexuales, el pudor es tendencia del ser humano a obrar en cuanto a las acciones de su cuerpo y de su sexo, de una manera limpia, pulcra y ordenada, con sujeción a los fines, funciones y naturaleza de su aparato reproductor de su impulso sexual.<sup>16</sup>

El profesor español Eloy Velasco Núñez establece cual es el problema transfronterizo del delito informático de la pornografía infantil y el Grooming, el identifica que las autoridades tienen un grave problema para controlar los delitos informáticos en los cuales encontramos como se vende y se traspasan la pornografía infantil, el problema que nace de esta información es la captura y judicialización de estos individuos esto lo afirma:

---

<sup>14</sup> Derecho Penal Sexual, Martínez Zúñiga, 1977.

<sup>15</sup> Manual de Derecho Penal, Pabón Parra, 2013

<sup>16</sup> Manual de Derecho Penal, Pabón Parra, 2013

El problema en los delitos informáticos es la peculiaridad de la circulación por donde rueda el objeto delictivo, que a diferencia de lo que ocurre en el mundo convencional, que al ser físico es de mayor fácil control, en el virtual, presenta precisamente la dificultad de que los agentes policiales puedan asegurar el debido control de lo que circula a través de las telecomunicaciones que se hacen por la Red. (Velasco, 2010, p. 12)

Eloy identifica también como el Estado no se quedó atrás en cuanto a la delincuencia transnacional informática organizada, y con esto llegaron a crear infiltraciones sencillas para el análisis e investigación de los Ciberdelincuentes que con las nuevas tecnologías comenzaron una organización delictiva informática.

Creándose también así el avance de la policía en cuanto a medios informáticos, a aquellos agentes infiltrados en las organizaciones transnacionales de pornografía infantil.

Por otra parte, es necesario proyectar la ampliación de la red del delito informático a nivel mundial en razón a que éste tiene su carácter extraterritorial en este sentido se trata de delincuencia transnacional.

Para hablar de delincuencia transnacional debemos entender su significado, el autor Francisco Milán<sup>17</sup> la determina así:

“Se trata de un grupo social con una cierta estructura y con miembros que se organizan para cometer acciones delictivas. A diferencia del delincuente que actúa en solitario, los individuos que forman parte de

---

<sup>17</sup> Sociedad Enferma o Estilo de Vida, Francisco Milán, 2016

una banda de delincuencia organizada deben responder a la estructura y cumplir con una determinada función.” (Milán, 2016, p.50)

La delincuencia organizada suele dedicarse a tareas más complejas que robos comunes o hurtos. Estos grupos de crimen organizado se involucran en actividades como el tráfico de drogas o armas, la trata de blancas, el contrabando o la falsificación.

Es habitual que estas organizaciones delictivas estén regidas por un orden jerárquico. Los miembros de las capas más bajas deben hacer méritos para ascender y mostrar su lealtad a los jefes.

El profesor Arrean Hernando Velasco Melo indica que para enfrentar a los delitos informáticos es necesario seguir un modelo como el de Inglaterra en materia de seguridad de la informática y que la mayoría de Estados deben tener avance significativo en la criptología debido a que el avance del sistema Británico de tecnologías, se beneficia con la criptología que es una disciplina científica que se dedica al estudio de la escritura secreta, es decir, estudia los mensajes que, procesados de cierta manera, se convierten en difíciles o imposibles de leer<sup>18</sup>.

La ciberdelincuencia transnacional actual con los nuevos tipos de lenguajes, crea redes para establecer una comunicación para una mayor seguridad ante las autoridades competentes y la organizaciones de pornografía infantil utilizan lenguajes secretos para llevar a cabo sus ventas de material pornográfico ilícito y así venderlos a otros países, formando una

---

<sup>18</sup> Tomado de El derecho informático y la gestión de seguridad de la información. Revista de derecho, Universidad del Norte. Melo, A. H. (2008)

terrible organización transnacional, que afecta drásticamente a millones de niños alrededor del mundo.

Dentro de las tendencias posmodernas de la criminología, encontramos la postulación del Derecho Penal del Enemigo o el enemigo en el derecho penal, concepción que pareciera influenciar la manera como se aborda la creación, la aplicación y ejecución de la norma penal.

La precitada construcción es sustentando por el excelso jurista alemán Gunther Jakobs en términos de la gran relación que tiene el Estado con sus ciudadanos, debido a que los clasifica de una manera desde una perspectiva contractualista<sup>19</sup>, en la cual los encasilla “Las personas y el enemigo”, debido a que aquella persona que infrinja o viole el contrato social que tiene el ciudadano con el Estado, prácticamente se vuelve enemigo del Estado, el filósofo francés Rousseau se refiere a la violación del contrato social, cuando la persona comete una acción punible y esta perjudica a la sociedad, Jakobs lo que hizo es una analogía refiriéndose al “enemigo” como aquella persona que quebranta el contrato social, que acepta al encontrarse en una determinada sociedad cobijada por un Estado.

El jurista alemán Jakobs también se sustenta en diferentes autores importantes como Hobbes y Kant para sustentar su tesis aclarando que tipo de personas son las que se les debe aplicar el derecho penal del enemigo, y precisamente son aquellos individuos que pueden en palabras de Hobbes cometer delitos de “Alta traición”<sup>20</sup> en contra del Estado, y en palabras de Kant personas que “Reinciden”<sup>21</sup> en la comisión de delitos como lo podemos observar en la siguiente cita:

---

<sup>19</sup> Contrato Social, Jean-Jacques Rousseau, 2005

<sup>20</sup> Derecho Penal del Enemigo, Gunther Jakobs y Cancio Meliá, 2003

<sup>21</sup> Derecho Penal del Enemigo, Gunther Jakobs y Cancio Meliá, 2003

HOBBS y KANT conocen un Derecho penal del ciudadano - contra personas que no delinquen de modo persistente, por principio- y un Derecho penal del enemigo contra quien se desvía por principio; éste excluye, aquél deja incólume el status de persona. El Derecho penal del ciudadano es Derecho también en lo que se refiere al criminal; éste sigue siendo persona. Pero el Derecho penal del enemigo es Derecho en otro sentido. Ciertamente, el Estado tiene derecho a procurarse seguridad frente a individuos que reinciden persistentemente en la comisión de delitos; a fin de cuentas, la custodia de seguridad es una institución jurídica. Más aún: los ciudadanos tienen derecho a exigir del Estado que tome las medidas adecuadas, es decir, tienen un derecho a la seguridad. (Jakobs, 2003, p.32)

El Derecho penal del enemigo persigue a los criminales más peligrosos que puedan afectar a la sociedad considerablemente, pero me parece necesario definir en palabras del penalista alemana Jakobs que significa el Derecho Penal del enemigo, consiste en sancionar la conducta de un sujeto peligroso en una etapa muy anterior a un acto delictivo, sin esperar a una lesión posterior tardía. Se sancionan la conducta y la peligrosidad del sujeto, y no sus actos. El mismo fenómeno se da en el ámbito procesal, especialmente con la restricción de algunos ámbitos privados. Por ejemplo, la posibilidad de allanamiento de morada con fines investigativos, la posibilidad de registro de viviendas o la instalación de micrófonos o instrumentos para escuchas telefónicas.<sup>22</sup>

El derecho penal del enemigo pena la conducta de un sujeto peligroso en etapas previas a la lesión, con el fin de proteger a la sociedad en

---

<sup>22</sup> Derecho Penal del Enemigo, Gunther Jakobs y Cancio Meliá, 2003

su conjunto, y esto quiebra la relación lógica tradicional entre pena y culpabilidad, dice. Sin embargo, aclara que él no hace otra cosa que describir la realidad, ya que el supuesto derecho penal ideal, para el cual todos somos iguales, contradice las medidas que los Estados adoptan con los sujetos altamente peligrosos.<sup>23</sup>

La teoría del Derecho Penal del enemigo, surgió desde el fatídico atentado terrorista del 11 de septiembre del 2001 en donde fue atacado el World Trade center, nace esta teoría penal, a razón para combatir a la delincuencia Transnacional organizada.

Pero hay que entender que se debe aplicar el Derecho Penal del Enemigo adecuadamente para no caer en un totalitarismo judicial, como lo podemos revalidar en las siguientes citas:

El Estado puede proceder de dos modos con los delincuentes: puede ver en ellos personas que delinquen, personas que han cometido un error, o individuos a los que hay que impedir mediante coacción que destruyan el ordenamiento jurídico. Ambas perspectivas tienen, en determinados ámbitos, su lugar legítimo, lo que significa al mismo tiempo que también pueden ser usadas en un lugar equivocado. (Jakobs, 2003, p.47)

En consecuencia, conforme a los lineamientos del Derecho Penal del Enemigo, las personas que cometen delitos de carácter sexual, se deben judicializar de manera más estricta, en virtud a que en la mayoría de los casos los delitos informáticos relacionados con la pornografía infantil, pertenecen a

---

<sup>23</sup> La imputación objetiva en derecho penal, Gunther Jakobs, 2011

un grupo de delincuencia transnacional organizada que reporta una serie de beneficios ilegales de carácter social y económico invaluable.



## 5. CAPITULOS

### 5.1. Capítulo uno: Generalidades de la Delincuencia Organizada Transnacional y Delito Informático de Pornografía Infantil.

#### 5.1.1 Generalidades de la Delincuencia Organizada Transnacional

La definición de la delincuencia transnacional la Comisión Europea en su acción común 98/733/JAI<sup>24</sup>, establece que es una sociedad estructurada jerárquicamente, de más de tres personas determinadas, que actúan de manera concreta, con el fin de cometer acciones punibles.

Con base a la mencionada acción común, las Naciones Unidas no se quedaron atrás al realizar una definición de la Delincuencia Organizada Transnacional como se puede observar en la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional que fue diseñada en el año de 2000, esta fue elaborada en el país de Italia en la región de Sicilia precisamente en la ciudad metropolitana de Palermo.

Esta convención constituye un tratado multilateral que tiene como objetivo contrarrestar la delincuencia organizada transnacional (DOT), este relevante documento contiene en su artículo (02) la siguiente dilucidación de la estructura y organización de la (DOT):

- a) Por “grupo delictivo organizado” se entenderá un grupo estructurado de tres o más personas que exista durante cierto tiempo y que actúe concertadamente con el propósito de cometer uno o más delitos graves

---

<sup>24</sup> Acción común de 21 de diciembre de 1998 adoptada por el Consejo sobre la base del artículo K.3 del Tratado de la Unión Europea, relativa a la tipificación penal de la participación en una organización delictiva en los Estados miembros de la Unión Europea.

o delitos tipificados con arreglo a la presente Convención con miras a obtener, directa o indirectamente, un beneficio económico u otro beneficio de orden materia [...] c) Por “grupo estructurado” se entenderá un grupo no formado fortuitamente para la comisión inmediata de un delito y en el que no necesariamente se haya asignado a sus miembros funciones formalmente definidas ni haya continuidad en la condición de miembro o exista una estructura desarrollada. (Naciones Unidas, P.13, 2010)

El grueso de los investigadores coincide en señalar al período de los años 20 y 30 en Estados Unidos de América como la cuna de la Delincuencia Organizada, tanto por la prohibición del alcohol, esto permitió que se comenzaran a establecer organizaciones, que se dedicaban a comercialmente alcohol, generando una serie de ganancias astronómicas en dólares, esto dio paso al mercado negro.

El mercado negro es aquel conjunto de actividades relacionadas con la compra y venta de mercancías y servicios que son ilícitos, como lo era el caso del alcohol en Estados Unidos, la delincuencia a raíz de generar mucho dinero, tiene que organizarse como empresa para continuar con recibir activos económicos, así que, realizaron una jerarquía organizacional donde cada persona tenga un aporte, realice y principalmente elabore una función determinante para lograr un objetivo, como lo era vender alcohol, pero con el paso del siglo XX, las organizaciones criminales no solo se dedicaron a vender alcohol, se dedicaron a delitos como el secuestro, homicidio, hurto, trata de personas, etc.

La historia nos ha demostrado a groso modo que organizaciones delictivas como “La cosa Nostra” “Los yakuza” “La mafia rusa” “Los carteles mexicanos”, establecieron una organización piramidal en donde desde la base

hasta la cabeza de la organización eran beneficiados por el dinero recogido por su actividad ilegal como lo establece el autor:

“La organización interna de La Cosa Nostra, era rígida y vertical, similar a una estructuración piramidal, de modo que los jefes podían ostentar un control y beneficio de las actividades ilícitas de los miembros subordinados, aún y cuando los primeros no participan directamente en tales actividades, es decir, las ganancias que aportaban los miembros inferiores a los jefes era una especie de diezmo o primicia, pese a ello todos los miembros dentro de la estructura piramidal resultaban beneficiados. (Mendoza, P.33, 2017)

Dentro de los cuadros de mando se encontraba La Comisión la cual constituye el órgano de mando de La Cosa Nostra y se encargaba de aprobar planes a realizar, dichas organizaciones antiguas que cometían se caracterizaban por los siguientes elementos que se puede observar en el siguiente párrafo:

Las características fundamentales de las Organizaciones son: a). - Organización funcional; cada miembro tiene una misión específica. b). - Permanencia; formada por un determinado número de personas, si llegare a falta un miembro, éste es reemplazado inmediatamente. c). - Jerarquía; uno o dos jefes solamente, y ésta se basa en la antigüedad. d). - División de trabajo; cada miembro tiene su tarea, y nadie hace el trabajo de otro, salvo en ocasiones que requieran inmediatez en la acción. e). - Profesionalización de sus miembros, sobre todo en la Delincuencia de los Balcanes; suelen ser Militares retirados o expulsados de sus ejércitos, así como el uso de profesionales para la apertura de Cajas Fuertes, etc. f). - Fin ilícito al que se le busca beneficios pecuniarios muy elevados, la constitución de delitos que le

lleven a ingresar importantes cantidades de dinero. (Covarrubias & del Carmen, 2007, págs. 7-8)

Pero con el paso del tiempo y las nuevas modalidades de delitos las organizaciones criminales se han desplazado a todos los lugares del mundo, y de esta forma se han creado diferentes redes de comunicación que han permitido su ocultamiento y continuidad de actividades ilegales lo que dificulta su persecución, toda vez que por tiempo indefinido, de manera concertada y sistematizada se asignan tareas y/o funciones con el fin de cometer delitos, el profesor Hamann nos dice lo siguiente:

(...) su amplia cobertura geográfica dificulta el trabajo de las autoridades, ya que al involucrar diferentes jurisdicciones nacionales se requiere la coordinación de múltiples agencias y oficinas de diferentes Estados. Así, un Estado puede ser exitoso en el desmantelamiento de un grupo criminal en su territorio, pero si otros grupos que hacen parte de la red continúan funcionando en otros Estados su desmantelamiento total es casi imposible. (...) (Hamann, 2008, p.8)

Existe una serie de características de la delincuencia organizada transnacional posmoderna que los docentes mexicanos explican en la siguiente aseveración donde detalla claramente los elementos para comprender como funciona una organización criminal transnacional:

Características de la delincuencia organizada contemporánea: a). - Utilización de redes comerciales internacionales. b). - Aprovechamiento del libre mercado; la apertura de las fronteras europeas les da un radio de acción amplísimo. c). - Expansión de actividades en otras áreas geográficas; pretenden construir en un territorio actividades delictivas que no existían. d). - Interrelación con otras organizaciones nacionales

e internacionales; unas se unen a otras, claro que, con beneficio para ambas, para el aprovechamiento del delito. e). - Reinversión de los beneficios; se trata del antiguo "trueque" cambiando acciones delictivas por otras y así obtener los beneficios ejemplo, una banda que roba vehículos de lujo para canjearlos por droga. f). - Tipologías delictivas g). - Relación entre delitos. (Covarrubias & del Carmen, 2007, págs. 7-8)

Un caso significativo de organización delictiva, la Mafia Rusa, que según especialistas aparece en la escena criminal después de la caída del bloque socialista, pero a decir verdad ya existía en décadas anteriores la mafia en general inclusive en los Estados Unidos practicando el tráfico de personas, así como el de armas; sin embargo, en la actualidad también trafican con materiales radioactivos, drogas, teniendo como escenario los países de Europa del Este y Rusia incluida.

Los avances vertiginosos de las TIC, la delincuencia comienza a inmiscuirse en la internet porque prácticamente encuentra más rentable la economía cibernética debido a su facilidad transnacional de los delitos, tanto por que a la policía se le hace difícil perseguir mediante la internet la comisión y ejecución de delitos informáticos, pero es necesario explicar que son los delitos informáticos y de donde provienen.

La ampliación del crimen se puede deber a la aparición de la comunicación de la red entre personas y el mercado de módems, terminales económicos, elementos tecnológicos, etc., que han sido utilizado por los Ciberdelincuentes para cometer diferentes acciones punibles.

La comunidad internacional identifico que la ciber criminalidad nacen con el objetivo de obtener capital ilegalmente, las organizaciones se

introdujeron en el mercado negro cibernético con ese fin y vieron la oportunidad con los delitos informáticos.

Las formas delictuales de la delincuencia globalizada internacional se han fortalecido y actualizado con las TIC (Tecnologías de la información y comunicación), estas son el conjunto de tecnologías desarrolladas para gestionar información y enviarla de un lugar a otro. Abarcan un abanico de soluciones muy amplio. Incluyendo las tecnologías para almacenar información y recuperarla después, enviar y recibir información de un sitio a otro, o procesar información para poder calcular resultados y elaborar informes" (Servicios TIC, 2006, P.25)

Estas organizaciones delictuales en el caso del delito de pornografía infantil se fundamentan en una división de trabajos para realizar la producción y comercialización del material ilícito, realizando diferentes actos con el de obtener un material específico para la comercialización claramente con la elaboración de la pornografía infantil por cualquier tipo de medio vulnera La integridad sexual al menor de edad que está siendo filmado o fotografiado, existe otras personas dentro de la organización que su función es buscar compradores o una serie de redes de comercialización en páginas virtuales, para que cualquier comprador alrededor del mundo pueda adquirir el material de contenido erógeno.

Dentro de la teoría del Joint Criminal Enterprise existe una relación con la delincuencia organizada transnacional, ya que dentro de esta postura se divide en tres categorías que son: perpetración directa, co-perpetración e indirecta perpetración, estos elementos nos permiten inferir en como en la comisión de la pornografía infantil tiene diferentes etapas como lo son conseguir la víctima para poder realizar el material, en una segunda etapa producir, elaborar y editar el material y finalmente la comercialización del

producto ilegal terminado, el común denominador permite asumir un agendamiento previo de voluntades en procura de un objetivo común, ejecutado directa o indirectamente.

### **5.1.2 Pornografía Infantil**

Los autores Morilla y Lorenzo nos explican cómo funcionan las divisiones y la comercialización de la pornografía infantil:

No obstante, lo más común es la integración de un equipo de personas cada una de las cuales ostenta unas funciones atribuidas –captación de niños, filmación de imágenes, fotografiado, publicidad [...] y supervisadas por un sujeto que actuaría de “coordinador”. A tal efecto, debe plantearse la siguiente regla proporcional: a mayor número de integrantes mayor calidad tendrá el sitio web referido pues se dispondrá de más y variado material. [...] c) Operan de forma permanente. Una vez insertado el contenido de la página lo que hacen es actualizarla introduciendo material nuevo cada cierto intervalo de tiempo. (Fernández & Lorenzo, 2005, pág. 120)

Una de las más importantes formas de cómo estas organizaciones se lucran es por el medio magnético que le depositan capital a realizar las comprar uno de los más claros ejemplos son las tarjetas de crédito y por el medio de transacciones por la moneda Bit Coin es una moneda, pero completamente digital. Es decir, se considera una divisa como el dólar y el euro, pero se centra en ser usada enteramente por internet, esta no utiliza ninguna transacción física.

La Bitcoin no depende de una entidad única y disfruta del anonimato completo a diferencia de los pagos que se están impulsando actualmente con

tarjeta de crédito. Como lo podemos encontrar en la siguiente cita (BTC, 2018): “Los bitcoins se puede intercambiar de forma casi instantánea por euros, dólares o cualquier otra moneda tradicional, y cada vez hay más comercios de todo tipo que lo aceptan como medio de pago.” El objetivo claramente de la acción ilícita que conlleva este delito informático es de beneficiar el patrimonio económico a través de la red, los autores Fernández y Lorenzo nos explican cómo funciona este comercio en la siguiente afirmación:

[...]e) Su objetivo es meramente económico. Como contraprestación a la adquisición de material pornográfico el destinatario debe abonar una cantidad de dinero. El pago de la misma puede realizarse a través de tarjetas de crédito –cuestión especialmente incómoda para el adquirente pues puede dejar rastro de su compra– en cuyo caso, una vez realizada la transferencia, el comprador recibirá una clave de acceso a la página en cuestión o recibirá las imágenes requeridas vía correo electrónico; o contra reembolso. (Fernández & Lorenzo, 2005, pág. 121)

La ciberdelincuencia transnacional actual con los nuevos tipos de lenguajes, crea redes para establecer una comunicación para una mayor seguridad ante las autoridades competentes y las organizaciones de pornografía infantil utilizan lenguajes secretos para llevar a cabo sus ventas de material pornográfico ilícito y así venderlos a otros países, formando una terrible organización trasnacional, que afecta drásticamente a millones de niños alrededor del mundo.

Otro obstáculo que de forma constante se plantea en los delitos cometidos por medio de internet es la transfronterización del conflicto, esto es, la conexión del hecho delictivo con el espacio y la soberanía de diferentes Estados como consecuencia de la vinculación espacial con los mismos del



hecho delictivo, lo que puede producirse por la colaboración de varios autores ubicados en diferentes Estados, la diferente localización de los servidores, la utilización de proxys en la navegación, la atomización de los resultados, ello plantea en la investigación diversos problemas como la determinación de la competencia internacional o la diversidad de legislaciones aplicables.

La pornografía infantil como delito sufre el problema de la transfronterización del comercio digital, debido a que los creadores y comerciantes del contenido erógeno, a través de las TIC tienen una facilidad de ocultamiento de la IP, a través de diferentes tipos de programas, esto permite que tanto los compradores y los vendedores puedan mantenerse en anonimato.

Este delito principalmente existe desde la primigenia de la red las personas que sufren pedofilia, que precisamente es una parafilia que consiste en la excitación o el placer sexual que se obtiene, principalmente a través de actividades o fantasías sexuales con niños de, generalmente, entre 8 y 12 años, las cuales son los principales compradores.

La pornografía infantil comprende una serie de requisitos que los establece la UNICEF:

Fotografías y videos que muestren a menores de edad sosteniendo relaciones sexuales o en poses sexualmente sugestivas.  
Fotografías y videos que muestren a personas mayores de edad que 'aparentan' ser niños o adolescentes y que tienen relaciones sexuales o están en poses sexualmente sugestivas.  
Las gráficas, caricaturas, anime y dibujos que muestren personajes infantiles o que representan a menores de edad manteniendo relaciones sexuales o en poses sugestivas.

Los autorretratos (o selfies) que muestren a menores de edad o personas que aparenten serlo en actividades sexuales. Imágenes de niñas y niños desnudos que estén en un ambiente con connotaciones sexuales. (Unicef, 2018, p. 15)

Las empresas criminales, para poder comercializar la pornografía infantil a través de la red, lo que hacen es comunicarse a través de ya sean grupos de diferentes redes sociales o con los correos electrónicos, con los compradores de dicho material.

Estas organizaciones delictuales se fundamentan en una división de los trabajos en donde una parte realiza el material ilícito realizando diferentes actos y vulnerando los derechos de la integridad sexual al menor de edad que está siendo filmado o fotografiado, existe otras personas dentro de la organización que su función es buscar compradores o una serie de redes de comercialización en páginas virtuales, para que cualquier comprador alrededor del mundo pueda adquirir el material de contenido erógeno.

Existe una serie de modalidades de La pornografía infantil que realmente no son punibles en la legislación colombiana la corte de suprema de justicia a través de la sentencia SP123-2018/45868 de febrero 7 de 2018 una serie de modalidades que son las siguientes.

B La pornografía técnica: es cuando en la escena interviene una persona con las mismas fisionomías de un menor de edad, es decir, simula ser un niño. En palabras de la Corte es cuando “intervienen personas que no tienen la condición de ser menores de edad, pero que aparentan serlo” .

C La pseudopornografía: es cuando se usan fotografías o imágenes de menores de edad en escenas pornográficas, pero “realmente los menores no fueron abusados” .

D La pornografía infantil artificial: cuando a través de dibujos o animaciones se crea un menor de edad en una escena pornográfica, “es decir, no representa un ser humano con existencia real”. Además, “no constituyen pornografía infantil las imágenes de niños en poses simplemente sugestivas” , señaló la Corte al explicar que existe un grupo de personas atraídas exclusivamente por los niños, a quienes dichas imágenes “resultan ser suficientes para llevarlos al camino de la excitación sexual” .

Uno de los medios de comercialización que es vigente y que las autoridades no han hecho una adecuada vigilancia es el videojuego Mmo Second Life, donde a pesar de los múltiples escándalos, continua con inconvenientes judiciales, debido a que ese videojuego posee muchísimas facilidades para la comercialización de la pornografía infantil y se puede observar en el caso alemán como se observa en el artículo periodístico “Germany investigates Second Life child pornography, que tiene más de 12 años, pero en este artículo explican que el videojuego es una puerta para que se comercialice la pornografía infantil.

La función que cumple Second Life con la comercialización de la pornografía infantil es que, a través de la creación de mundos, estos escenarios virtuales, se encuentran encriptados y protegidos, y se pueden transferir cualquier tipo de archivo, documento, fotografía, videos etc.

En las salas las personas pueden pasar cualquier tipo de información lo que no se encuentra vigilado debido a que los administradores de Second

Life, dejan a libre disposición de las personas, transmitir la información que ellos quieran.

Así es como de esta manera a través de Second Life, los comercializadores de pornografía infantil logran comercializar el contenido erótico ilegal.

La autora Georgina explica en su tesis que el Second Life se puede recrear cualquier tipo de escenario, casas, monumento etc., donde las personas pueden compartir cualquier tipo de información como lo asevera en la siguiente cita: “La lista de posibilidades dentro de Second Life no tiene fin, desde el diseño y la construcción de una obra arquitectónica hasta compartir poesía en directo con un grupo de personas, conocidas o no, de todo el mundo.” (Georgina, 2016, p.102), Second Life ha sido uno de los sitios que hasta hace más de 8 años no ha sido investigado por las autoridades internacionales, como la ECPAT.

## **5.2. Capítulo dos: regulación del delito informático de pornografía infantil**

El abordaje del delito informático de pornografía infantil, amerita presentar la evolución y reconocimiento de los Derechos de los Niños, tanto como en el contexto nacional como internacional.

### **5.2.1. Instrumentos de derecho internacional**

#### ***De la Declaración Universal de los Derechos del Niño***

El antecedente más distante se encuentra en la Declaración de Derechos del Niño, firmado en Ginebra, en 1924. Se establece que la humanidad debe otorgar al niño lo mejor que se pueda brindar para que crezca en un entorno y condiciones seguras, sin ningún tipo de discriminación y se erigen cinco principios básicos encaminados a proteger las condiciones esenciales para el pleno desarrollo del menor.

Estos principios son el establecimiento de condiciones adecuadas para el desarrollo de manera normal material y espiritual. La atención alimentaria, de salud, de amparo frente a dificultades es el segundo principio. El socorro en caso de calamidad, la protección ante la explotación y la educación para el servicio son los siguientes principios planteados.

El día 20 de noviembre de 1959, la Asamblea General de Naciones Unidas renovó la Declaración de Derechos del Niño de inicialmente planteada en 1924 y emitió diez principios básicos en lo que denominó “Declaración de los Derechos del Niño de 1959”. En esta, se ampliaron los principios mencionados anteriormente y se añadieron los de comprensión y al amor de los padres y de la sociedad, protección, tratamiento y unidad familiar.

Mediante esta reafirmación universal de los derechos del niño se exaltó al menor como un ser humano al que se le debe tener propiciar unas condiciones de desarrollo físico, moral, mental, social, espiritual, con libertad y dignidad.

Como consecuencia de la Segunda Guerra Mundial, El 10 de diciembre de 1948, se aprobó y proclamó la Declaración Universal de Derechos Humanos por la Asamblea General de Naciones Unidas, orientada a reconocer los derechos y libertades de las personas.

### ***Del Pacto Internacional de Derechos Civiles y Políticos***

En esta declaración, se hace alude a la infancia en el artículo 25.2 al delimitar que «la maternidad y la infancia tienen derecho a cuidados y asistencias especiales. Todos los niños, nacidos de matrimonio o fuera de matrimonio, tienen derecho a igual protección social». De conformidad con ello, la familia, debe recibir la protección y asistencia básica para asumir a plenitud sus responsabilidades en la sociedad.

El 16 de diciembre de 1966, se firma el Pacto Internacional de Derechos Civiles y Políticos en el que, pese a ser un texto general, se distinguen derechos de la infancia. En el artículo 24 se mencionan los principios de no discriminación, inscripción y nacionalidad:

“Todo niño tiene derecho, sin discriminación alguna por motivos de raza, color, sexo, idioma, religión, origen nacional o social, posición económica o nacimiento, a las medidas de protección que su condición de menor requiere, tanto por parte de su familia como de la sociedad y del Estado. Todo niño será inscrito inmediatamente después de su

nacimiento y deberá tener un nombre. Todo niño tiene derecho a adquirir una nacionalidad.” (Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos Ginebra, Suiza, 1966)

### ***De la Convención de los Derechos del Niño***

El 20 de noviembre de 1989, se firma la Convención de Derechos del Niño -Tratado internacional de las naciones Unidas- en sus 54 artículos, a Convención, declara que los niños y niñas, son sujetos con derecho de completo crecimiento físico, mental y social, y expresan de manera libre sus opiniones.

Adicionalmente, el Tratado compila todos los derechos y libertades reconocidos en los menores de edad. Algunos de los derechos reconocidos en ella, tratan de: la libertad de expresión; el bienestar; la unidad familiar; supervivencia y desarrollo; la formación; protección a la vida privada, entre otros.

Durante la mayoría del siglo XX fueron de suma importancia en el reconocimiento y establecimiento de los derechos de los niños y niñas, fruto de una creciente y visible vulnerabilidad en la que se encontraban los menores y de la comprensión y necesidad de protección y entornos seguros que en su momento las organizaciones y sociedad consideraron necesarios.

A partir de la última década del siglo XX enceta la lucha por la prevención de la criminalidad contra los menores. En la Cumbre Mundial en favor de la infancia celebrado en New York en 1990, se establecen las

Directrices para la Prevención de la Delincuencia Juvenil<sup>25</sup> (Directrices de Riad).

Las Directrices de Riad, definen estrategias dirigidas a prevenir tanto la criminalidad juvenil y como la protección en situación de alto riesgo social. Incita a los gobiernos a establecer políticas que orienten al menor a ser útiles en la sociedad con criterio humanista y, así mismo, a que se creen las condiciones de oportunidad para que ello suceda.

Deberá reconocerse la necesidad y la importancia de aplicar una política progresista de prevención de la delincuencia, así como de estudiar sistemáticamente y elaborar medidas pertinentes que eviten criminalizar y penalizar al niño por una conducta que no causa graves perjuicios a su desarrollo ni perjudica a los demás. La política y las medidas de esa índole deberán incluir: a) La creación de oportunidades, en particular educativas,[...]; b) La formulación de doctrinas y criterios especializados para la prevención de la delincuencia, [...]; c) Una intervención oficial que se guíe por la justicia y la equidad, y cuya finalidad primordial sea velar por el interés general de los jóvenes; d) La protección del bienestar, el desarrollo, los derechos y los intereses de todos los jóvenes; e) El reconocimiento del hecho de que el comportamiento o la conducta de los jóvenes que no se ajustan a los valores y normas generales de la sociedad [...]; f) La conciencia de que, según la opinión predominante de los expertos, calificar a un joven de "extraviado", "delincuente" o "predelincuente" a menudo contribuye a que los jóvenes desarrollen pautas permanentes de comportamiento indeseable". (Asamblea General, 1990)

---

<sup>25</sup> Proclamadas por la Asamblea General de las Naciones Unidas en su resolución 45/112, de 14 de diciembre de 1990.



En 1995 se crea la Red de Información de los Derechos del Niño (Child Rights International Network, CRIN) cuyo aporte es la investigación, política e incidencia a partir de la protección de los Derechos del Niño.<sup>26</sup>

La OIT (Organización Internacional del Trabajo) en 1999, acoge el Convenio sobre las Peores Formas del Trabajo Infantil donde se prohíbe cualquier trabajo que afecte la salud, la moral y la seguridad de los niños y niñas.

Está demostrado que finalizando el siglo XX, se empezaron a identificar nuevos problemas que atañen a la indefensión de los niños y niñas, no bastó con reconocerlos como sujetos de derecho, pensantes y sintientes, sino, que además se empieza a ver la necesidad de protegerlos de los nuevos retos a los que se enfrenta tras la globalización y modernidad. Así pues, en el nuevo siglo XXI tiene nuevos desafíos que resolver frente a la protección y dignidad de los niños.

### ***Protocolos facultativos de la convención de los derechos del niño***

El año 2000 Inicia con la extensión de la Convención de los Derechos del Niño, a través de dos Protocolos Facultativos en los que los Estados de Naciones Unidas, se comprometen a tomar las medidas necesarias para que los niños y niñas no sean parte de conflictos armados, ni sean explotados, vendidos o abusados sexualmente.

Dos Protocolos Facultativos de los Derechos del niño más se celebraron: El primero, trata sobre procedimientos relativos a las

---

<sup>26</sup><https://home.crin.org/>

comunicaciones, donde el Comité de los Derechos del Niño (CDN) puede presentar denuncias de violaciones de estos derechos y llevar a cabo investigaciones (2011). El segundo, la Convención sobre los Derechos del Niño es ratificada por Somalia y Sudán del Sur.

El reconocimiento de los Derechos de los Niños, es una base fundamental para prevenir y sancionar todos aquellos delitos que se cometen en contra de los niños y niñas, sin embargo, con la evolución de la tecnología se han desatado otro tipo de abusos contra los niños y niñas.

Las regulaciones de los delitos informáticos en algunos Estados no son completamente claras y, hace que exista cierta impunidad frente a su comisión. En los siguientes acápite se verifica la comisión de los delitos informáticos referente a la pornografía Infantil.

#### **5.2.2. Delito Informático.**

Las organizaciones internacionales han desarrollado diferentes normativas y tratados para contrarrestar el delito informático teniendo en cuenta que la comisión de estos es trasciende fronteras.

Debe destacarse que la Organización de las Naciones Unidas (ONU), en el marco del Octavo Congreso sobre Prevención del Delito y Justicia Penal, firmado en 1990 en Cuba, incita a los Estados a modernizar sus legislaciones penales para que las nuevas figuras delictiva tengan una sanción, por otra parte, incita a que incluyan nuevos procedimientos de investigación y probatorios con los recursos tecnológicos.

En 1995 la ONU lanza el Manual Sobre la Prevención y Control del Delito Informático y, con el resalta la importancia de una definición uniforme y

armonía de procedimientos procesales para tratar los delitos informáticos entre los Estados.

Por su parte, la Unión Europea frente a este fenómeno, lanza dos programas que promueven la cultura, mejora y superación de obstáculos jurídicos de la información<sup>27</sup>.

La OCDE en 1986 publicó un informe titulado Delitos de Informática, aquí se analizó las propuestas de reforma a la normativa jurídica de los Estados parte, junto a su normativa actual. La propuesta naciente, estableció un Listado mínimo de usos indebidos de la informática para que los Estados mismos tuviesen en cuenta para penalizar.

En este listado se encontraban delitos como el fraude y la falsificación, sabotaje informático, la alteración de datos y programas de los ordenadores, obstrucción o acceso no autorizado.

Además, en 1992, la OCDE presentó un conjunto de normas para reforzar la seguridad en los sistemas de información, ofreciendo así los cimientos para que los Estados pudieran fundar un marco de seguridad para sus sistemas informáticos.

Por último, el Consejo de Europa ha emitido varias Recomendaciones<sup>28</sup> a los Estados parte con el fin de armonizar las leyes nacionales e internacionales sobre la criminalidad informática.

---

<sup>27</sup> Los programas titulados (Information Market Policy Action Plan) IMPACT

<sup>28</sup> Recomendación N° R (81)12; Recomendación N° R (81)20; Recomendación N° R (89)9. Recomendación N° R (95)13

Las organizaciones internacionales se han visto en la obligación de gestionar nuevas normas tendientes a descongestionar los problemas derivados del uso de la red de internet y de las nuevas tecnologías. Por esta razón se han creado nuevas figuras delictivas como lo es la estafa informática, Cyber-crime o delitos informáticos.

### **5.2.3. instrumentos de derecho interno**

En Colombia, el Código Penal <sup>29</sup>, regula en (pocos artículos) las conductas se realizan mediante la utilización indebida de los medios informáticos, los cuales se presentan a continuación:

Artículo 195. Acceso abusivo a un sistema informático. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa.

Artículo 199. Sabotaje. El que con el fin de suspender o paralizar el trabajo destruya, inutilice, haga desaparecer o de cualquier otro modo dañe herramientas, bases de datos, soportes lógicos, instalaciones, equipos o materias primas, incurrirá en prisión de uno (1) a seis (6) años y multa de cinco (5) a veinte (20) salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena mayor.

Si como consecuencia de la conducta descrita en el inciso anterior sobreviniere la suspensión o cesación colectiva del trabajo, la pena se aumentará hasta en una tercera parte

---

<sup>29</sup> Ley 599 de 2000

Artículo 219-A. Utilización o facilitación de medios de comunicación para ofrecer servicios sexuales de menores. El que utilice o facilite el correo tradicional, las redes globales de información, o cualquier otro medio de comunicación para obtener contacto sexual con menores de dieciocho (18) años, o para ofrecer servicios sexuales con estos, incurrirá en pena de prisión de diez (10) a catorce (14) años, y multa de sesenta y seis (66) a setecientos cincuenta (750) salarios mínimos legales mensuales vigentes.

Las penas señaladas en el inciso anterior se aumentarán hasta en la mitad (1/2) cuando las conductas se realizaren con menores de catorce (14) años"

Artículo 270. *Violación a los derechos morales de autor.* Incurrirá en prisión de dos (2) a cinco (5) años y multa de veinte (20) a doscientos (200) salarios mínimos legales mensuales vigentes quien:

1. Publique, total o parcialmente, sin autorización previa y expresa del titular del derecho, una obra inédita de carácter literario, artístico, científico, cinematográfico, audiovisual o fonograma, programa de ordenador o soporte lógico.
2. Inscriba en el registro de autor con nombre de persona distinta del autor verdadero, o con título cambiado o suprimido, o con el texto alterado, deformado, modificado o mutilado, o mencionando falsamente el nombre del editor o productor de una obra de carácter literario, artístico, científico, audiovisual o fonograma, programa de ordenador o soporte lógico.

3. Por cualquier medio o procedimiento compendie, mutile o transforme, sin autorización previa o expresa de su titular, una obra de carácter literario, artístico, científico, audiovisual o fonograma, programa de ordenador o soporte lógico.

Parágrafo. Si en el soporte material, caratula o presentación de una obra de carácter literario, artístico, científico, fonograma, videograma, programa de ordenador o soporte lógico, u obra cinematográfica se emplea el nombre, razón social, logotipo o distintivo del titular legítimo del derecho, en los casos de cambio, supresión, alteración, modificación o mutilación del título o del texto de la obra, las penas anteriores se aumentarán hasta en la mitad.

Artículo 271. *Defraudación a los derechos patrimoniales de autor.* Incurrirá en prisión de dos (2) a cinco (5) años y multa de veinte (20) a mil (1.000) salarios mínimos legales mensuales vigentes quien, salvo las excepciones previstas en la ley:

1. Por cualquier medio o procedimiento, sin autorización previa y expresa del titular, reproduzca obra de carácter literario, científico, artístico o cinematográfico, fonograma, videograma, soporte lógico o programa de ordenador, o transporte, almacene, conserve, distribuya, importe, venda, ofrezca, adquiera para la venta o distribución, o suministre a cualquier título dichas reproducciones.

2. Represente, ejecute o exhiba públicamente obras teatrales, musicales, fonogramas, videogramas, obras cinematográficas, o cualquier otra obra de carácter literario o artístico sin autorización previa y expresa del titular de los derechos correspondientes.

3. Alquile o de cualquier otro modo comercialice fonogramas, videogramas, programas de ordenador o soportes lógicos u obras cinematográficas, sin autorización previa y expresa del titular de los derechos correspondientes.

4. Fije, reproduzca o comercialice las representaciones públicas de obras teatrales o musicales, sin autorización previa y expresa del titular de los derechos correspondientes.

5. Disponga, realice o utilice, por cualquier medio o procedimiento, la comunicación, fijación, ejecución, exhibición, comercialización, difusión o distribución y representación de una obra de las protegidas en este título, sin autorización previa y expresa de su titular.

6. Retransmita, fije, reproduzca o por cualquier medio sonoro o audiovisual divulgue, sin autorización previa y expresa del titular, las emisiones de los organismos de radiodifusión.

7. Recepciones, difunda o distribuya por cualquier medio, sin autorización previa y expresa del titular, las emisiones de la televisión por suscripción.

Parágrafo 1. Si como consecuencia de las conductas contempladas en los numerales 1, 3 y 4 de este ARTICULO resulta un número no mayor de cien (100) unidades, la pena se rebajará hasta en la mitad.

Parágrafo 2. Adicionado por el art. 36, Ley 1915 de 2018.

Artículo 272. Violación a los mecanismos de protección de los derechos patrimoniales de autor y otras defraudaciones. Incurrirá en multa quien:

1. Supere o eluda las medidas tecnológicas adoptadas para restringir los usos no autorizados.
2. Suprima o altere la información esencial para la gestión electrónica de derechos, o importe, distribuya o comunique ejemplares con la información suprimida o alterada.
3. Fabrique, importe, venda, arriende o de cualquier forma distribuya al público un dispositivo o sistema que permita descifrar una señal de satélite cifrada portadora de programas, sin autorización del distribuidor legítimo de esa señal, o de cualquier forma de eludir, evadir, inutilizar o suprimir un dispositivo o sistema que permita a los titulares del derecho controlar la utilización de sus obras o producciones, o impedir o restringir cualquier uso no autorizado de estos.
4. Presente declaraciones o informaciones destinadas directa o indirectamente al pago, recaudación, liquidación o distribución de derechos económicos de autor o derechos conexos, alterando o falseando, por cualquier medio o procedimiento, los datos necesarios para estos efectos. (Ley 599, 2000)

Se hace necesario especificar los artículos que el código penal le dedica al uso debido de los medios informáticos en razón a que aquí se puede observar de manera directa que no hay una tipificación de los delitos informáticos, no hay una caracterización directa de ello en parte porque se considera que la informática no es en sí la comisión de un delito sino, el medio para hacerlo. Es por ello que en el siguiente apartado se hará énfasis sobre la pornografía infantil como delito en el Estado Colombiano.



Pérez Luño, menciona que la noción genérica del delito Informático es “aquel conjunto de conductas criminales que se realicen a través del ordenador electrónico, o que afecten al funcionamiento de los sistemas informáticos” (Pérez Luño, 1996). En efecto, este concepto puede representar lo que para la jurisprudencia colombiana significa el delito informático.

#### **5.2.4. Regulación de la Pornografía Infantil.**

Los entes reguladores de los Estados frente a la definición de delito informático pueden presentar vacíos de carácter técnico y jurídico, sin embargo, esto ha ido evolucionando hasta el punto de llegar a la clasificación de los delitos informáticos en cuatro grupos criminológicos a saber: Infracciones a la Intimidad; ilícitos en el ámbito económico; ilícitos de comunicación telemática; Otros ilícitos informáticos. (Suárez Sánchez, 2009)

En el presente apartado, se desarrolla a fondo el grupo ilícitos de comunicación telemática especialmente la regulación de la pornografía infantil, toda vez que este grupo trata de la información de contenido racista o de apología a la violencia y difusión de material pornográfico infantil, entre otros, con la ayuda de ordenadores a través de sistemas telemáticos, a través de internet. (Suárez Sánchez, 2009)

A continuación, se enuncian las regulaciones internacionales que hacen frente a la comisión del delito de pornografía infantil:

- Resolución del Parlamento Europeo (1997), Comunicación de la Comisión sobre la lucha contra el turismo sexual que afecta a niños.

- ONU 2000, Protocolo facultativo de la Convención sobre los Derechos del Niño relativo a la venta de niños, la prostitución infantil y la utilización de niños en la pornografía.
- Convenio 185, del Consejo de Europa, sobre la Ciberdelincuencia realizada en Budapest en 2001.
- Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual, celebrado en Lanzarote en el año 2007. Ratificado por el BOE 274, del 12 de noviembre de 2010.
- 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 transnacional. Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, el Fondo de las Naciones Unidas para la Infancia y la Organización Internacional para las Migraciones (2000).

La regulación de la pornografía infantil a nivel internacional empezó unos años antes de recibir el nuevo siglo XXI, tras el reconocimiento de los Derechos de los Niños y toda la red de acción que se entramó para su garantía y protección.

En la legislación colombiana se integran los instrumentos normativos internacionales a través de la Constitución Política de Colombia de 1991 en su artículo 44, en concordancia con los artículos 34 y 35 de la Convención sobre los Derechos de Niño de 1989, asevera lo siguiente:

Artículo 44. Son derechos fundamentales de los niños: la vida, la integridad física, la salud y la seguridad social, la alimentación

equilibrada, su nombre y nacionalidad, tener una familia y no ser separados de ella, el cuidado y amor, la educación y la cultura, la recreación y la libre expresión de su opinión. Serán protegidos contra toda forma de abandono, violencia física o moral, secuestro, venta, abuso sexual, explotación laboral o económica y trabajos riesgosos. Gozarán también de los demás derechos consagrados en la Constitución, en las leyes y en los tratados internacionales ratificados por Colombia.

La familia, la sociedad y el Estado tienen la obligación de asistir y proteger al niño para garantizar su desarrollo armónico e integral y el ejercicio pleno de sus derechos. Cualquier persona puede exigir de la autoridad competente su cumplimiento y la sanción de los infractores. Los derechos de los niños prevalecen sobre los derechos de los demás. (C.P.C., 1991)

Conforme a lo anterior, la legislación colombiana tipifica los delitos de acceso carnal abusivo con persona menor de catorce años, así como, acto sexual con persona menor de catorce años, de la siguiente manera<sup>30</sup>:

*Artículo 208. Acceso carnal abusivo con menor de catorce años.* El que acceda carnalmente a persona menor de catorce (14) años, incurrirá en prisión de cuatro (4) a ocho (8) años.

*Artículo 209. Actos sexuales con menor de catorce años.* El que realizare actos sexuales diversos del acceso carnal con persona menor de catorce (14) años o en su presencia, o la induzca a prácticas sexuales, incurrirá en prisión de tres (3) a cinco (5). (Ley 599, 2000)

---

<sup>30</sup> Ley 599 de 2000 Código Penal Colombiano.

En concordancia con el Protocolo Facultativo de la Convención sobre los Derechos del Niño referente a la venta de niños, prostitución infantil y uso de niños en la pornografía, el legislativo tipificó el delito de pornografía con personas menores de 18 años, sancionando en el Código Penal Colombiano Ley 599 de 2000 en los artículos 218 y 219 relacionados a continuación:

Artículo 218. El que fotografíe, filme, grabe, produzca, divulgue, ofrezca, venda, compre, posea, porte, almacene, trasmita o exhiba, por cualquier medio, para uso personal o intercambio, representaciones reales de actividad sexual que involucre persona menor de 18 años de edad. Igual pena se aplicará a quien alimente con pornografía infantil bases de datos de Internet, con o sin fines de lucro.

Artículo 219A. Utilización o facilitación de medios de comunicación para ofrecer actividades sexuales con personas menores de 18 años. El que utilice o facilite el correo tradicional, las redes globales de información, telefonía o cualquier medio de comunicación, para obtener, solicitar, ofrecer o facilitar contacto o actividad con fines sexuales con personas menores de 18 años de edad. (Ley 599, 2000)

El Estado Colombiano también ha sancionado la Ley 679 de 2001, estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución. Esta ley también dispone la promoción de sistemas de autorregulación respecto a las redes globales de información. Así mismo, prohibiciones, deberes y sanciones a proveedores o servidores, administradores y usuarios, respecto al alojamiento de vínculos o material de tipo pornográfico, el desarrollo de un sistema de información sobre delitos sexuales contra el infante, la vigilancia y

control, así como la capacitación al personal de la policía y la investigación estadística.

En la Ley 679 de 2001 se resalta el esfuerzo por prevenir la comisión del delito de pornografía infantil en su Artículo 5 sanciona lo siguiente:

Artículo 5. Informe de la comisión. Con base en el informe de que trata el artículo anterior, el Gobierno nacional, con el apoyo de la Comisión de Regulación de Telecomunicaciones, adoptará las medidas administrativas y técnicas destinadas a prevenir el acceso de menores de edad a cualquier modalidad de información pornográfica, y a impedir el aprovechamiento de redes globales de información con fines de explotación sexual infantil u ofrecimiento de servicios comerciales que impliquen abuso sexual con menores de edad. (Ley 679, 2001)

En desarrollo del Artículo 5 presentado anteriormente, el Estado sanciona el Decreto 1524 de 2002 cuyo objeto es:

[...] Establecer las medidas técnicas y administrativas destinadas a prevenir el acceso de menores de edad a cualquier modalidad de información pornográfica contenida en Internet o en las distintas clases de redes informáticas a las cuales se tenga acceso mediante redes globales de información.

Así mismo a propender para que estos medios no sean aprovechados con fines de explotación sexual infantil u ofrecimiento de servicios comerciales que impliquen abuso sexual con menores de edad.”

Por último, se menciona el Código de Infancia y Adolescencia<sup>31</sup> en el que se expiden las normas para la protección integral de los niños, niñas y adolescentes en el ejercicio de sus derechos y libertades. Describe su finalidad en el primer artículo de la siguiente manera:

Artículo 1º. Finalidad. Este Código tiene por finalidad garantizar a los niños, a las niñas y a los adolescentes su pleno y armonioso desarrollo para que crezcan en el seno de la familia y de la comunidad, en un ambiente de felicidad, amor y comprensión. Prevalecerá el reconocimiento a la igualdad y la dignidad humana, sin discriminación alguna.

En el Artículo 20 del Código de Infancia y Adolescencia, se menciona la pornografía como uno de los Derechos de Protección, a los que accede el menor en Colombia. Por otra parte, en el Artículo 47 del mismo Código, especta que los medios de comunicación deben: “Abstenerse de realizar transmisiones o publicaciones que atenten contra la integridad moral, psíquica o física de los menores, que inciten a la violencia, que hagan apología de hechos delictivos o contravenciones, o que contengan descripciones morbosas o pornográficas”.

Finalmente, el Código de Infancia y adolescencia en las funciones que asigna a la Policía Nacional, labores de inteligencia para combatir redes dedicadas a la a la distribución y comercialización de pornografía infantil a través de internet o cualquier otro medio, además, de adelantar labores de vigilancia a fin de controlar el tráfico de material pornográfico.

---

<sup>31</sup> Ley 1098 de 2006

### **5.3. Capítulo tres: Modalidades de Pornografía Infantil en Colombia: la Informática como Medio de Masificación Delincuencial.**

#### **5.3.1. Caracterización de la pornografía infantil en Colombia.**

De acuerdo al documento Criterios de Clasificación de Contenidos de Pornografía Infantil en Internet<sup>32</sup>, La pornografía infantil en Colombia se presenta en las siguientes modalidades:

- Grooming en línea: Seducción en red. Acciones por medio de las cuales una persona busca una relación engañosa en internet con un niño, una niña o adolescente, con el propósito de conocerlo y volverlo más vulnerable a contactos y abusos sexuales. Estos contactos pueden darse en cualquier espacio virtual o dispositivo utilizado por una persona menor de 18 años, con mayor frecuencia, son llevados a cabo por medio del uso de cámaras web o intercambio de imágenes y textos eróticos o sugestivos (factores que permiten divulgar el material en redes de abusadores y explotadores) y, buscan mediante el chantaje, tener encuentros personales para cometer el abuso sexual físico o el envío de más material propio o ajeno. Los lugares que facilitan a los abusadores realizar el grooming son, entre otros, las salas de chat, las redes sociales y la mensajería instantánea.
- Sexting (envío de contenidos eróticos): Acciones por medio de las cuales las personas envían imágenes o textos de naturaleza sexual provocativa, sugestiva o explícita, a través de mensajes o fotos en los celulares u otros dispositivos digitales

---

<sup>32</sup> Publicado por el Instituto Colombiano de Bienestar Familiar en 2016.

(computadores, tabletas, entre otros). Generalmente el material es compartido voluntariamente por un niño, una niña o adolescente con otro, con quien tiene un compromiso afectivo o sentimental; en muchas ocasiones este material es compartido por el destinatario, sin el debido consentimiento, con muchas otras personas, cuando el compromiso se rompe o la relación es engañosa. La publicación del material autogenerado usualmente es problemática, con riesgos que permanecen en el tiempo y puede tener consecuencias devastadoras. Además, el material sexual puede ser usado para extorsionar a la víctima, pidiéndole recursos, acciones, o más material a cambio de privacidad.

- Sextorsión: Explotación sexual en la cual la persona que envía material sexual a través del sexting es chantajeada con su propio material con el fin de obtener dinero o algún otro beneficio por parte del chantajista. El chantaje consiste en la amenaza de publicar el material en internet o ser enviado a los y las familiares y conocidos(as) de la persona implicada. (Instituto Colombiano de Bienestar Familiar, 2016)

Estos conceptos se actualizan cada dos años según lo ordenado por la Ley 679 de 2001.

Además, clasifica la pornografía infantil según los materiales o contenidos y según el fin de la siguiente manera:

*Según los materiales o contenidos:*

- Pornografía leve o suave: en este tipo de pornografía no hay actividad sexual explícita, pero implica imágenes desnudas, “seductoras e insinuantes”



de niñas, niños o personas con aspecto de niños, niñas y adolescentes. Incluye la exhibición de estos en distintas posturas eróticas, pero no su participación en ningún comportamiento explícitamente sexual.

- Pornografía dura o fuerte: consiste en la exhibición de acceso carnal, actos sexuales explícitos, o ambos, en los que participen niños, niñas, adolescentes o personas con indicios de ser menores de 18 años (Ruiz 1999)

*Según el fin:*

- Pornografía comercialmente producida con fines de lucro.
- Pornografía producida para ser circulada e intercambiada.
- Pornografía utilizada con otros fines delictivos (chantaje, trata, etc.).
- Pornografía producida para consumo exclusivamente personal, entre otros.

El Grupo de Información de Criminalidad de Delitos Sexuales de la Policía Nacional de Colombia, en Colombia sancionan las siguientes Modalidades de Pornografía Infantil además de las mencionadas anteriormente: Redes peer to peer, Aplicaciones maliciosas, pague por ver, ciberacoso Y la explotación sexual infantil como mercado criminal (servicios y material digital).

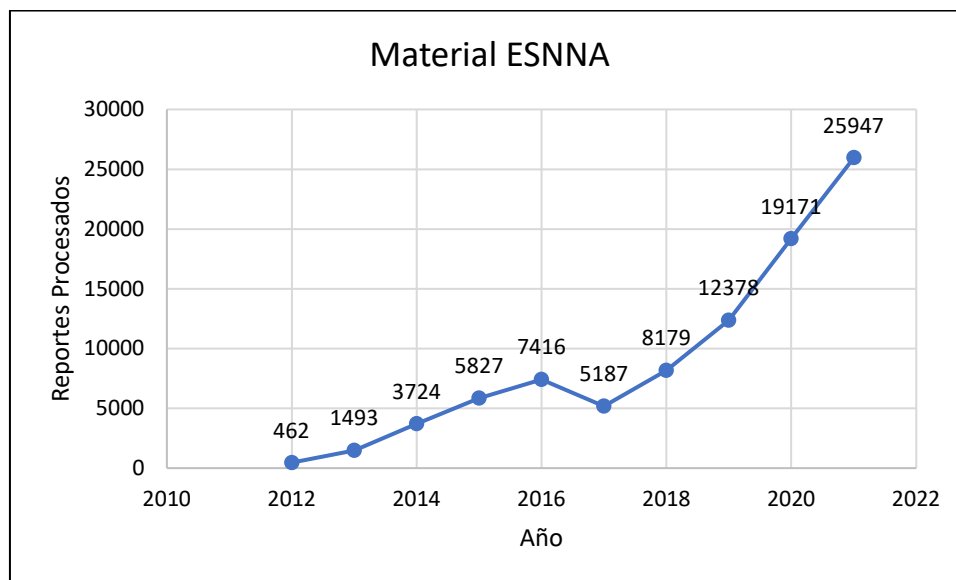
### **5.3.2. Estadísticas de la Pornografía infantil en Colombia.**

En el presente acápite se realiza una aproximación al delito de la pornografía infantil a través de estudios y registros que entidades públicas y organizaciones no gubernamentales han precisado a través de la sistematización de los datos reportados a estas entidades.

Los delitos relacionados con la Explotación Sexual Comercial de Niños Niñas y Adolescentes -ESCNNA- se empezaron a registrar luego de la formalización de la Política Pública para la Prevención y Erradicación de la Explotación Sexual Comercial de niñas, niños y adolescentes.<sup>33</sup>

La Organización Te Protejo<sup>34</sup>, ha recopilado información sobre los casos reportados en Colombia, desde al año 2012. La categorización de la información es sobre: Material ESNNA, ESCNNA, Ciberacoso, intimidación escolar, Maltrato, trabajo y abuso, Venta de alcohol y otras SPA, Contenidos inapropiados, entre otros. Para el estudio aquí convenido, se analizará el Material ESNNA (Explotación Sexual de Niños, Niñas y Adolescentes) Y ESCNNA (Explotación Sexual Comercial de Niños, Niñas y Adolescentes)<sup>35</sup>.

Gráfico 1. Material ESNNA



Fuente: Documento Técnico: Te protejo (2021). Elaboración propia.

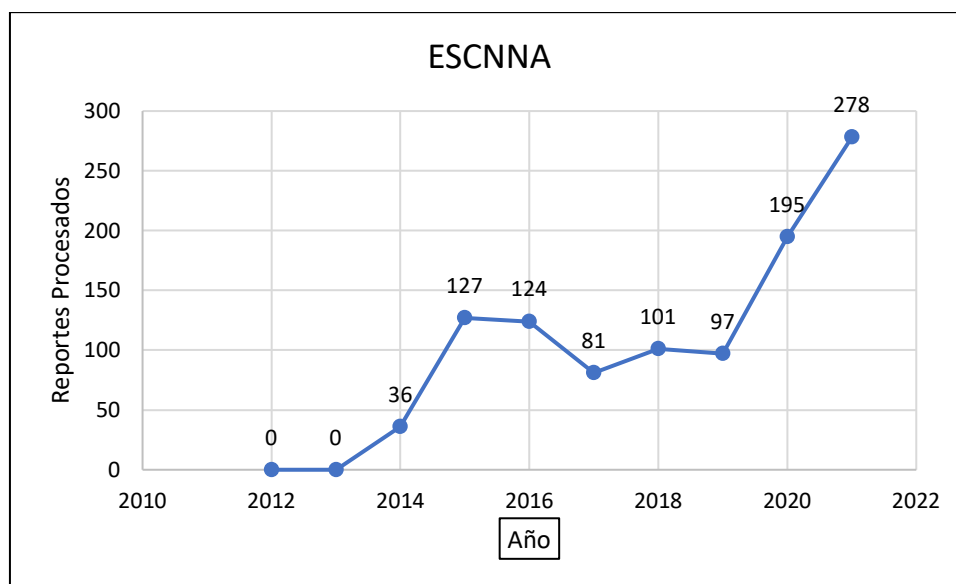
<sup>33</sup> Véase Ley 1336 de 2009

<sup>34</sup> Canal de denuncia virtual que reúne el reporte de contenidos ilegales, principalmente, pornografía, abuso y explotación sexual en la infancia y adolescencia a través de internet o cualquier herramienta TIC.

<sup>35</sup> Informe técnico: Te protejo 2021

A partir del año 2018 los casos procesados sobre Material ESNNA ha triplicado, en los años 2020 y 2021 (fecha coincidente con la pandemia) los reportes sobrepasaron las diez mil casos siendo esto, una cifra alarmante.

Gráfico 2. Explotación Sexual Comercial de Niños, Niñas y Adolescentes



Fuente: Documento Técnico: Te protejo (2021). Elaboración propia

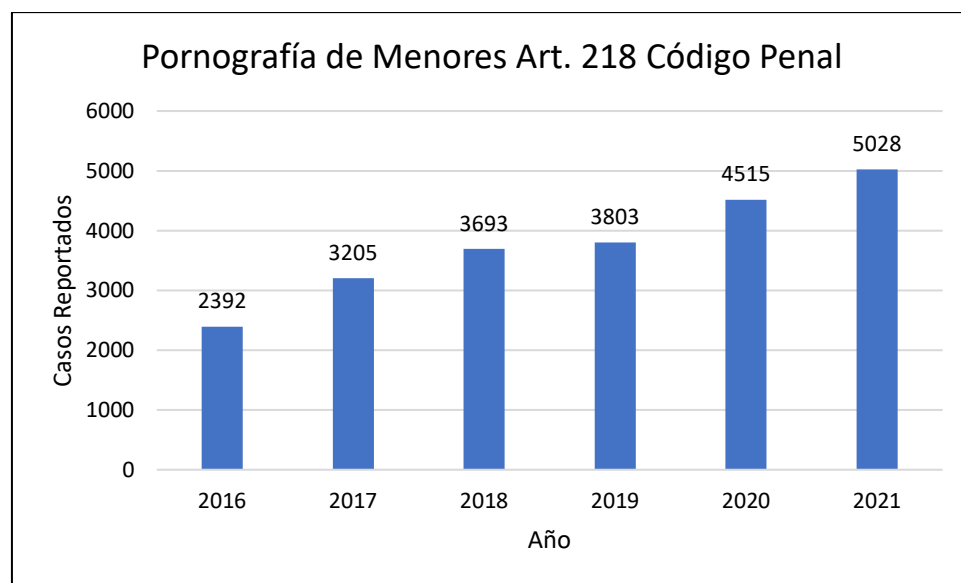
En la estadística de Explotación Sexual Comercial de Niños, Niñas y Adolescentes (ESCNNA), el reporte presenta un comportamiento similar a la estadística anterior, es decir, hay una correlación entre la producción de Material ESNNA y la ESCNNA.

En el Documento Técnico se aclara que estos casos reportados son principalmente de las siguiente ciudades: el 51% de los mismos se realizaron desde la ciudad de Bogotá y los departamentos de Antioquia, Cundinamarca y Valle del Cauca. Hasta la fecha (2021) no han recibido reportes desde

Guaviare, San Andrés, Vaupés y Vichada y no se recibieron reportes de nuevos municipios.

La Fiscalía General de la Nación, presenta estadísticas de denuncia por delitos en concordancia con el Código Penal Acusatorio. En ella se realizó una comparación de casos reportados en los últimos seis años y coincide con las estadísticas de denuncias virtuales (no en cifras) en el sentido de un aumento que para el caso presentado en el gráfico siguiente se trata de la duplicidad de los casos que se presenta al año 2021.

Gráfico 3. Estadística de denuncia por delitos.



*Fuente: Fiscalía General de la Nación (2021). Elaboración propia.*

El aumento de las cifras ha generado controversia en el mando legislativo colombiano quienes han convocado a debates de control político a las entidades del Estado competentes para reevaluar la implementación de medidas contra la ESCNNA. Este aumento de casos ha sido a nivel mundial:

La recesión causada por el COVID-19 ha impactado directamente en el riesgo de ocurrencia en los delitos de ESCNNA por el incremento de menores de edad con necesidades económicas y conflictos familiares derivados de la actual crisis, factores de riesgo que son aprovechados por los tratantes de personas y explotadores sexuales quienes, según investigaciones, adelantan estos crímenes preferiblemente en ciudades que gozan de reconocimiento turístico, cultural e histórico. (Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC),2021)

#### **5.4. Capítulo cuatro: Alternativa Regulatoria de Prevención Contra la Proliferación de la Pornografía Infantil**

Considerando que en los Tratados no existe ninguna política comunitaria propia para la punición del delito informático de pornografía infantil. Así mismo, que se debe ampliar la cobertura de los tratados e invitar a aquellos países que no hacen parte de ellos a que colaboren para contrarrestar el crimen.

La gran dificultad del control de la red de Internet favorece la comisión del crimen, ya que, a través de esa red, se puede difundir gratuitamente material de pornografía infantil, así como, obtener información sobre la oferta de pornografía con plena libertad.

Además, la publicidad incontenible y escueta de estas prácticas perversas, no sólo conduce a la trivialización de los crímenes cometidos contra los niños, sino que, además incita a que más consumidores se sumen a este negocio.

Queda expuesto que hay que batallar con la oferta y la demanda al mismo tiempo y, que cualquier medida que se tome de manera unilateral no será suficiente para contrarrestar el crimen.

La prostitución y pornografía infantil aumenta con más ahínco en los países con mayor pobreza. Se está transformando cada vez más en un problema global, ya que estos países se encaminan a otras fuentes ilícitas para subsistir, además, que por lo general estos países no cuentan con normatividad sancionatoria fuerte para estos delitos.

Ante lo expuesto anteriormente, se propone una alternativa regulatoria que fortalezca el sistema judicial y legislativo en Colombia para prevenir la proliferación de la pornografía infantil. En los pilares a tratar:

Se procede a una adaptación importante de la conceptualización del delito informático relacionado a la información y a fraudes informáticos, así mismo, se refiere a la vulneración de la intimidad de las personas.

De acuerdo a lo expuesto en los capítulos, la legislativa Colombia “no se ha visto en la necesidad” de adaptarse legalmente a las normas internacionales sobre el delito informático de pornografía infantil, empero, la actualización normativa es necesaria para estar a un mismo nivel de confrontación del delito que permita tener instrumentos jurídicos para el alcance la punición del delito trascienda fronteras.

Se insta al legislativo colombiano a que haga balance de la legislación penal desde el punto de vista, la pornografía infantil y la trata de seres humanos, y a que, si fuere necesario, presente propuestas sobre los elementos constitutivos de los delitos y que incluya el principio de la extraterritorialidad y prescindan del requisito de la punibilidad bilateral.

Aunado a lo anterior es fundamental implementar el concepto jurisdicción penal universal o cosmopolita como primera alternativa en el sentido que independientemente del lugar ubicado geográficamente o en el extenso mundo de la internet todos los Estados tengan jurisdicción o competencia para judicializar la cibercriminalidad y en especial del delito informático de pornografía infantil. El lugar virtual extraterritorialidad ampliada implementarlo de tratados de instrumentos fuerza vinculante. Cualquier persona que cometa este tipo de infracciones bajo ninguna circunstancia se vea amparado por inmunidades fueros.

La jurisdicción penal universal la explica el profesor Bassiouni de la siguiente forma:

“la jurisdicción universal puede ser ejercida por un Estado sin ninguna conexión o vínculo jurisdiccional entre el lugar de la comisión, la nacionalidad del perpetrador, la nacionalidad de la víctima y el Estado que la ejercita. La base es, en consecuencia, exclusivamente la naturaleza del crimen<sup>30</sup> y el propósito es exclusivamente la reforzar el orden global, garantizando que se responda por la perpetración de ciertos crímenes. Precisamente debido a que un Estado que ejerce la jurisdicción universal lo hace en representación de la comunidad internacional, éste debe colocar los intereses generales de la comunidad internacional por encima de los suyos propios.” (Bassiouni, 2001, p.7)

A su vez se debe adoptar disposiciones extraterritoriales que faciliten la investigación, persecución y sanción a los individuos que hayan cometido delitos en materia de explotación sexual de niños en el extranjero.

Por otra parte, y apelando al Artículo 209 de la Constitución Política de Colombia, se debe hacer respetar el principio de coordinación y colaboración para que las autoridades competentes gestionen y consoliden los sistemas informativos contra el delito de pornografía infantil, evitando reprocesos informativos, de gestión y administrativos y fortaleciendo la red de apoyo, prevención y sanción de la pornografía infantil.

En la tercera medida, se plantea la creación de una política pública de carácter criminal que haga frente a la sensibilización y concientización de los nacionales y residentes en la dignificación del ser humano y la protección del



indefenso, con la finalidad de propagar el respeto por el otro y la cultura del cuidado humano.

Finalmente, es necesario establecer en Colombia una política criminal sólida que obstruya la acción del victimario, de ejemplo de castigo y tenga alcance transnacional.

El maestro alemán Gunther Jakobs nos establece que es necesario aplicar en una política criminal una serie de medidas más estrictas las cuales los abogados Bernardo y Mónica nos establecen en la siguiente cita:

Las medidas que un Estado inicia adoptando para dirigirse a un Derecho penal del enemigo son: - Construcción de tipos penales en los que se presenta un adelantamiento sustancial del momento en que el autor ha de ser sancionado. Ello se presenta con aquellas conductas en que no necesariamente se lesionan bienes jurídicos, sino que basta con la puesta en peligro abstracta de los mismos. - La desproporción entre la respuesta punitiva, especialmente entre delitos de lesión y los de peligro. - La restricción de garantías procesales, con especial énfasis en aquellos que protegen la esfera de la libertad. (Bernardo y Mónica, 2011, p. 24)

De conformidad con lo anterior, es fundamental que el Estado al implementar una política criminal bastante estricta que pueda ser aplicada en el territorio colombiano, de esta forma exista una adecuada persecución y judicialización a los ciberdelincuentes.

Las estadísticas están un gran aumento como se planteo en paginas posteriores

## 6. CONCLUSIONES

Los organismos internacionales se han dedicado a dar parámetros orientadores para el establecimiento armónico de leyes que castiguen el delito informático en los Estados, sin embargo, no existe el establecimiento de una red Jurídica que afiance y fortalezca los estados frente al delito informático de pornografía infantil.

La economía nacional e internacional afecta de manera directa la comisión de los delitos y mas aquellos que tienen que ver con el lucro. La incidencia de estos delitos está fuertemente marcada en las ciudades principales en razón a que en ella se concentra la distribución de la economía además de el acceso a la red de internet.

Gobierno de Colombia y las Organizaciones No Gubernamentales, se han aliado estratégicamente para ofrecer a los residentes, herramientas para manifiesten y/o denuncien ante las autoridades competentes los delitos por medio de portales tecnológicos, asesorías especializadas en conductas que atentan contra el bienestar sexual.

Existe una brecha tecnológica entre el área rural y urbana del territorio colombiano, razón por la cuál hay un vacío informativo de la comisión del delito de pornografía infantil en las zonas rurales. El hecho de que en la zona rural no haya conexión de red de internet no implica que en estas zonas no haya comisión del delito.

El delito informático en Colombia está orientado hacia la comisión de actos ilícitos que atenten a la información virtual y/o fraudes o estafas que se realizan en la informática.

La política criminal existente en contra de esta acción punible mencionada no ha surtido un verdadero efecto debido a que en materia tecnológica y de persecución las entidades de la mayoría de estados, no tienen material suficiente tecnológico para perseguir a los cibberdelincuentes, por lo cual las naciones ha sido inoperantes debido a que no ha aportado los recursos y no han consolidado una adecuada política criminal, que contrarreste la conducta punible ya mencionada, porque es un delito que afecta a una gran población infantil.

## 7. REFERENCIAS

### 7.1. Referencias Documentales

Año, B. V. (2006). Las nuevas tecnologías y delitos informáticos. La Habana: Tono Revista técnica de la Empresa de Telecomunicaciones de Cuba S.A.

Bonilla-Castro, E., & Rodríguez Sehk, P. (2005). Más allá del dilema de los métodos. Bonilla-Castro, E., y Rodríguez Sehk, P. Más allá del dilema de los métodos. La investigación en Ciencias Sociales. Colombia: Norma.

Barrera Mendoza, A. R., Rico Hernández, K. L., & Romero López, A. (2017). Identificación de factores de riesgo y protectores que inciden la vinculación de los niños, niñas y adolescentes en grupos de delincuencia organizada, de los grados sexto y séptimo del colegio Carlos Ramírez París.

De la Fuente, R. C., Erena, S. G., & González, A. V. (2013). *Sistema de ofuscación de malware para la evasión de NIDS*.

Delgado, S & França, O (2014). Flujo de material pornográfico infantil online, estudio exploratorio en 10 países de América Latina con foco en Uruguay. *Ciencias psicológicas* 8(1). 55-67.

Álvarez, V. M. (2007). *Virus Informáticos*. Coruña: Universidad de Coruña.

Canto, E. R. (2002). *Delincuencia Informática*. Barcelona: Comares.

Fiscalía General de la Nación. (2018). *Estructura de la Fiscalía General de la Nación*.

Informática, G. d. (2002) *Internet Comercio Electrónico & Telecomunicaciones*. Bogotá: Universidad de los Andes.

Instituto Colombiano de Bienestar Familiar. Lineamiento técnico de modalidades para la atención de niños, niñas y adolescentes, con derechos inobservados, amenazados o vulnerados. Resolución 1520 de febrero 23 de 2016.

Jakobs, G. (2011). *La imputación objetiva en derecho penal*. Bogotá: Universidad del Externado.

López, R. M. (2012). *Lecciones de Derecho Penal, Procedimiento Penal, y Política Criminal*. Bogotá: Biblioteca Jurídica DIKE.

Manzanera, L. R. (1981). *Criminología*. México D, F: Purrua, S.A.

Martínez, J. H. (1997). Colombia, El delito contra el patrimonio económico en Colombia.

Martínez, J. H. (1997). El delito Contra el Patrimonio económico en Colombia.

Maya, R. P. (2006). Aproximación a la criminalidad informática en Colombia. Universidad de los andes facultad de derecho.

Melo, A. H. (2008). El derecho informático y la gestión de seguridad de la información. Revista de derecho, Universidad del Norte.

Melía, G. J. (2003). Derecho Penal del Enemigo. Bogotá D.C: Thomson Civitas.

Milán, F. J. (2016). Sociedad Enferma o Estilo de Vida. Barcelona: Bloomington.

Monroy, B. E. (2002). La infancia y juventud explotada en Colombia. Bogotá: Universidad Javeriana.

Núñez, E. V. (2010). Entregas, Vigiladas y agente cubierto en internet. Justicia, Revista de Derecho Procesal.

Ojeda-Pérez, J. E. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. Cuadernos de contabilidad.

Organización para la Cooperación y el Desarrollo Económico [OCDE] (2014), Recomendación del Consejo de la OCDE relativa a la Cooperación

Internacional en el marco de investigaciones y procedimientos en materia de competencia. Aprobada por el Consejo el 16 de septiembre de 2014, México

Parra, L. O. (2012). Delitos informáticos (en el ciber espacio). Bogotá: Ediciones jurídicas Andrés Morales.

Parra, A. P. (2013). Manual de Derecho Penal. Bogotá D.C: Ediciones Doctrina y Ley.

Ríos, J. R. (2009). Delito electrónico en Colombia. Cali: Universidad Santiago de Cali.

Rivera-Morales, R. (2008). Los medios informáticos: tratamiento procesal. Universidad de la sabana.

Rosseau, J.-J. (2005). El contrato Social. Melsa: Mestas ediciones.

Ruiz, J. E. (2008). Delitos Informáticos en México. México D, F: IJF.

Ruedas Marrero, M., Ríos Cabrera, M. M., & Nieves, F. (2009). Hermenéutica: la roca que rompe el espejo. *Investigación y postgrado*, 24(2), 181-201.

Sabino, C. (1992). El proceso de la investigación. Buenos Aires: Panamericana.

Sánchez, A.S. (2009), LA ESTAFA INFORMÁTICA, Bogotá D.C: Ibáñez

Sanclemente, M. d. (2012). La protección de datos en el entorno laboral. *Revista de Derecho Comunicaciones y nuevas tecnologías*.

Taque, M. P. (2006). Delito en el comercio electrónico. Revista de Derecho de la universidad de Montevideo.

Hamman J. E (2008). Redes Criminales Transnacionales: Principal amenaza para la seguridad internacional en la posguerra fría.

Hita, A. R. (2010). La Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y sus protocolos complementarios: introducción a la problemática, contenidos normativos y conclusión. *Nómadas. Critical Journal of Social and Juridical Sciences*, 26(2).

Bernardo C. G Y Mónica C. C (2011) Derecho Penal del Enemigo

Veiga de Cabo, J., & Zimmermann Verdejo, M. (2008). Modelos de estudios en investigación aplicada: conceptos y criterios para el diseño. *Medicina y seguridad del trabajo*, 54(210), 81-88.

## 7.2. Documentos Electrónicos.

Convenio N° 185, del Consejo de Europa, sobre la Ciberdelincuencia (Convenio de Budapest). Recuperado de: [https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/20810/5/Convenio%20N%20185%20del%20Consejo%20de%20Europa%20sobre%20la%20Ciberdelincuencia%20\(Convenio%20de%20Budapest\).pdf](https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/20810/5/Convenio%20N%20185%20del%20Consejo%20de%20Europa%20sobre%20la%20Ciberdelincuencia%20(Convenio%20de%20Budapest).pdf)

Fiscalía General de la Nación. (2022). Estadística de denuncia por delitos. Recuperado de: <https://www.fiscalia.gov.co/colombia/gestion/estadisticas/delitos/>

ICBF. (2004) Criterios de clasificación de páginas en Internet con contenidos de pornografía infantil. Recuperado de: <https://www.ilo.org/ipeinfo/product/download.do?type=document&id=11137>

OCDE, (2016) Table 5.4 - ICT Readiness and Intensity Sub-Dimension: Cybercrime legislation and private sector co-operation indicator scores. Recuperado de: [https://www.oecd-ilibrary.org/development/competitiveness-in-south-east-europe/ict-readiness-and-intensity-sub-dimension-cybercrime-legislation-and-private-sector-co-operation-indicator-scores\\_9789264250529-table92-en](https://www.oecd-ilibrary.org/development/competitiveness-in-south-east-europe/ict-readiness-and-intensity-sub-dimension-cybercrime-legislation-and-private-sector-co-operation-indicator-scores_9789264250529-table92-en)

Centro Informático Ayudaley que define el polimorfismo. Recuperado de: <https://ayudaleyprotecciondatos.es/2021/04/29/malware-polimorfico/>

### **7.3. Referencias Jurisprudenciales**

Asamblea General ONU - Resolución A/RES/54/263 del 25 de mayo de 2000.

Convenio 182 sobre la prohibición de las Peores Formas de Trabajo Infantil y la Acción Inmediata para su Eliminación 1999.

Convención de los Derechos del Niño. 1989 Ratificada por ley 12 de 1991.

Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional – 15 de noviembre de 2000.



Protocolo Facultativo de la Convención de los derechos de la niñez, relativo a venta, prostitución y pornografía, Ratificado por Colombia a través de la Ley 765 de 2002.

Protocolo para la Prevención, Supresión y Castigo del Tráfico de Personas, Mujeres y Niños que complementa a la Convención de las Naciones Unidas sobre la Delincuencia Transnacional Organizada, PALERMO Ratificado el 25 de diciembre de 2003 por ley 800 DE 2003

Constitución Política de Colombia 1991

*Código Penal*, Ley 599 de 2000.

Ley 679 de 2001

Decreto 1524 de 2002. Por el cual reglamenta el artículo 5o. de la Ley 679 de 2001

Ley 1098 de 2006 - Código de Infancia y Adolescencia.

Ley 1098 de 2006. Por la cual se expide el Código de la Infancia y la Adolescencia”