LOS DERECHOS FUNDAMENTALES DE LAS VICTIMAS DE LOS CIBERDELITOS EN COLOMBIA

THE FUNDAMENTAL RIGHTS OF CYBERCRIME VICTIMS IN COLOMBIA

ANGELICA MARIA RAMIREZ CAMACHO
amramirezcamach@poligran.edu.co

NICOLE STEFAN RAMIREZ RAMIREZ
niramirez8@poligran.edu.co

LUIS DAVID MESA VELANDIA
ldmesav@poligran.edu.co

INSTITUCIÓN UNIVERSITARIA POLITÉCNICO GRANCOLOMBIANO
DERECHO
COLOMBIA

Agradecimientos

Primero que todo a Dios y nuestras familias por siempre apoyarnos y guiarnos en nuestro camino.

A la Doctora Johanna Marcela Lopera Narváez, tutora del artículo, por su ayuda y guía durante la realización de este.

A la Institución Universitaria Politécnico Grancolombiano por todas las enseñanzas que nos dieron en el transcurso de nuestra carrera.

Y, por último, pero no menos importante para la Universidad de Salamanca, debido a lo conocimientos brindados durante el diplomado de Derechos y Nuevas Tecnologías.

Resumen

A partir del momento en que una persona se encuentra en el internet, es susceptible a sufrir cualquier tipo de ataque o violación, vulnerando bienes jurídicos como la integridad, el patrimonio, la privacidad, etc., y esto a causa en gran medida de la capacidad con la se puede gestionar cualquier amenaza o riesgo, no obstante con la evolución de la tecnología, los ciberdelincuentes se preparan cada vez más con el objetivo de poder materializar un delito informático sin ser detectado, de hecho un delito cibernético es toda acción antijurídica que realiza una persona en el internet o cualquier otro medio informático**,** sin embargo los ciudadanos se encuentra amparados bajo leyes, reglas y normas que los ampara**.** El desarrollo del presente artículo permite determinar ¿cuáles son los derechos que se ven vulnerados en la comisión de los ciberdelitos? . Si existe una regulación, control y gestión de quienes infringen la ley y utilizan los portales en internet para atentar contra el patrimonio, la integridad y la dignidad humana violando la seguridad que se pueda tener al navegar en redes. Analizar cada referente de infractores e incautos e identificar, si existe una tendencia de personas más vulnerables que otras. Se optó por hacer uso y de acuerdo a la revisión de la literatura de la investigación descriptiva con enfoque cualitativo que se limita a tomar como referencia las cifras y valorarlas, pero sin ningún fin de atribuirles estandarización de estos datos, la investigación descriptiva permite realizar una descripción de una situación y del fenómeno logrando obtener información acerca del qué, cómo, cuándo y dónde, relativo al objeto de estudio. En cuanto a la regulación establecida entre España y Colombia se identifican similitud en los preceptos que regulan ambos países en su contenido normativo pues ambas a la firma del convenio de Budapest, coinciden en las mismas conductas y sanciones que han sido infringidas. Establecer controles de regulación y sanciones de los delitos informáticos reduciría el reporte de estafas, delitos sexuales y aportaría seguridad financiera para los internautas lo cual permitiría fortalecer el manejo de transacciones más seguras y mayor descongestión de trámites presenciales

Palabras Claves: Ciberdelitos, internet, leyes, ciberespacio, normas.

Summary

From the moment a person is on the internet, they are susceptible to any type of attack or violation, violating legal rights such as integrity, assets, privacy, etc., and this depends largely on the capacity with which you can manage any threat or risk, however with the evolution of technology, cybercriminals are increasingly preparing with the aim of being able to materialize a computer crime without being detected, in fact a cyber crime is any unlawful action carried out a person on the internet or any other computer medium, however citizens are covered by laws, rules and regulations that protect them. The development of this article makes it possible to determine what are the rights that are violated in the commission of cybercrimes? If there is regulation, control and management of those who break the law and use internet portals to undermine the heritage, integrity and human dignity, violating the security that can be had when browsing networks. Analyze each referent of offenders and unwary and identify, if there is a trend of more vulnerable people than others. It was decided to use and according to the literature review of descriptive research with a qualitative approach that is limited to taking the figures as a reference and evaluating them, but without any purpose of attributing standardization of these data to them, descriptive research allows a description of a situation and the phenomenon, obtaining information about what, how, when and where, relative to the object of study. Regarding the regulation established between Spain and Colombia, similarities are identified in the precepts that regulate both countries in their normative content, since both at the signing of the Budapest agreement coincide in the same behaviors and sanctions that have been infringed. Establishing controls in the regulation and sanctions of computer crimes would reduce the reporting of scams, sexual crimes and would provide financial security for Internet users, which would allow strengthening the management of safer transactions and greater decongestion of face-to-face procedures.

Keywords: Cybercrime, internet, laws, cyberspace, rules.

Introducción

La aparición de los delitos en el espacio cibernético ha planteado nuevos desafíos al derecho tradicional.

> "Este nuevo escenario delictivo exhorta a la doctrina especializada a plantearse si son adecuadas para la ciberdelincuencia las respuestas penales creadas para cubrir el espacio físico tradicional. Son solo muestras de ello las novedosas características técnicas, lógicas y de uso de las TIC (Tecnologías de la Información y la Comunicación), la cuestión de la cifra negra en los ciberdelitos, la contribución de la víctima desde un plano victimológico, la reinterpretación de las reglas espaciotemporales, la superior capacidad lesiva de estos injustos o la pluralidad de potenciales víctimas existentes"**.** (Gorostidi, 2020, párr. 5)

Desde el momento en que se entra al ciberespacio ya sea desde un celular, un televisor inteligente o un reloj, toda persona es vulnerable de convertirse en una posible víctima de los ciberdelincuentes, debido a que este espacio brinda muchas oportunidades para que se materialice un ciberdelito.

Sin embargo, según datos del Centro de Cibernética Policial (2017), "en los últimos 3 años se han recibido 15.565 incidentes informáticos a través de la plataforma proporcionada" (p. 12). Desde ciudadanos comunes hasta grandes empresas de los sectores público y privado, las opciones de las víctimas han cambiado, lo que ha traído mayores beneficios a las actividades delictivas. Sin embargo, Colombia no está familiarizado con este enfoque. Su característica principal es el fraude de Chief Executive Officer -CEO o director ejecutivo- en el cual los ciberdelincuentes adulteran el correo electrónico administrativo de la organización para iniciar la transferencia de fondos a sus cuentas, no obstante, se estima que cada caso de ataques fraudulentos por compromiso del correo electrónico empresarial que afecte a Colombia costará 130.000 dólares

Como dijo Pons (2017) los delitos tipificados como ciberdelitos son: fraude, hurto, chantaje, falsificación y malversación de fondos públicos. Del mismo modo, también se han interpuesto otros delitos derivados de la tecnología de la información y la comunicación, como es el caso del acoso, divulgación de información, la interferencia ilegal con datos y los delitos contra la propiedad, abuso sexual a través de Internet entre otros.

La presente investigación parte de la necesidad de poder comprender como se ven afectados los derechos de las víctimas de los ciberdelitos en Colombia, tales como la protección de datos, la seguridad financiera, el patrimonio y hasta la sexualidad entre otros.

A partir del análisis jurídico pertinente de acuerdo con la legislación colombiana y española. Así mismo se pretende establecer la población con mayor índice de vulnerabilidad frente a los ciberdelitos, si existe un rango de edad establecido o si los cibernautas oscilan con reiteradas conductas o portales que los vuelven más vulnerables que otros, frente al uso y consumo de las redes.

Y finalmente evaluar las leyes que tipifican actualmente los ciberdelitos en Colombia y España y por último, contrastar la normativa existente sobre los ciberdelitos en España y Colombia. Establecer un derecho comparado entre ambas legislaciones que permita analizar si Colombia cuenta con la normatividad suficiente para la regulación y

sanción en la comisión de la conducta punible.

Marco Jurídico

Establecer la población con mayor índice de vulnerabilidad frente a los ciberdelitos

El ciberbullyng, la pornografía, sextorsión, sexting y el grooming son tendencia en las redes sociales. Según el Centro Cibernéutico Policial (2017), “esta forma afecta principalmente al 75% de los niños, niñas y adolescentes, teniendo en cuenta que son más vulnerables al engaño y más vulnerables en el ciberespacio”. Asimismo, ha surgido otro fenómeno delictivo, el ciber espionaje, que afecta a todo lo concerniente. con la seguridad de la información teniendo esto una amplia gama de repercusiones en el sector económico (Pons, 2017). Por ello, “en un entorno altamente globalizado y competitivo, las grandes empresas multinacionales también son hostigadas por espías electrónicos para buscar información sobre nuevos proyectos de desarrollo” (Ruiz, 2016, p. 14).

Es importante mencionar que la TicTac (2019) concluyó que el hurto a través de medios informáticos es el que ocupa el primer puesto de denuncias en Colombia (31 058 casos); seguido por infracción a información personal (8037) y el acceso inapropiado y sin previo consentimiento (7994 acusaciones). Asimismo, último, dentro de esta lista, cabe mencionar las transferencias involuntarias de activos (3425). Por último, el uso de virus o software malicioso (2387).

Sin duda, la causa de que este delito aumente puede darse debido al desarrollo de las mismas ciudades. La alta población trae consigo una utilización continua del internet, situación que favorece a los delincuentes, quienes se enfocan en las pymes, organizaciones financieras y grandes compañías.

De acuerdo con el CCIT (La Cámara Colombiana de Informática y Telecomunicaciones) (2019), Business E-mail Compromise (BEC) es una de las principales amenazas para la cadena de suministro, que es una parte esencial de las actividades diarias de la empresa. Casi el 90% de los ciberataques a empresas colombianas se atribuyen a la ingeniería social.

A continuación, se muestra un marco de las principales modalidades de engaño en el 2019:

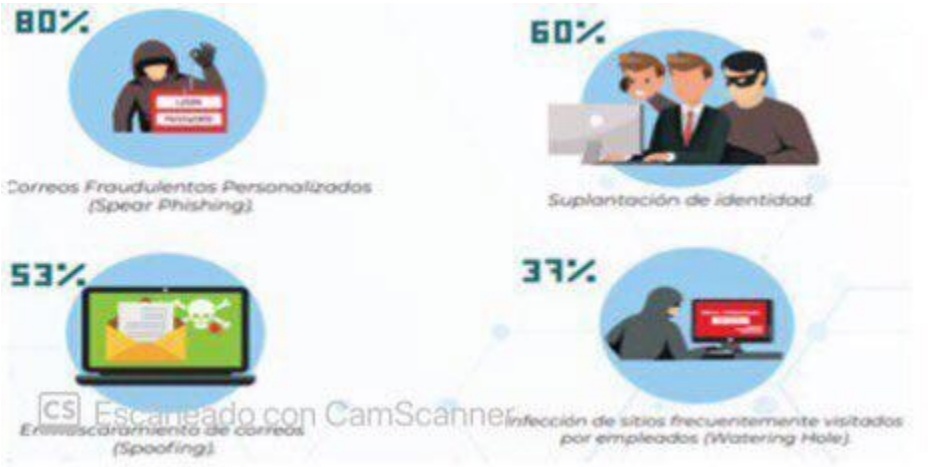

Figura 1. CCIT (2020). Tendencias de cibercrimen bajo mayor modalidad

Fuente: (TicTac, 2019)

Dentro de este contexto, Torres-González (2015), según su investigación, afirmó que existe una inclinación de que las empresas sean focos de atención en cuanto a este tipo de delitos. Entre muchos casos, debido al descuido en cuanto a seguridad de la información por parte de la misma entidad. Por lo mismo, se deben subsanar las fallas del sistema de seguridad para evitar la intromisión de desconocidos a los datos de las entidades.

Desde otra perspectiva, la Interpol (2020) aseveró que el internet, más específicamente, las llamadas ahora redes sociales se han vuelto una red de atracción para atrapar a nuevas víctimas de explotación sexual. Lo que ha favorecido que aumente el envío y transferencia de imágenes de menores. Incluso, el ciberbullying a nivel mundial oscila entre el 10-40 %. Sumado a esto, la situación actual también ha favorecido que este delito permanezca vigente. No cabe duda de que la falta de madurez tanto física y mental convierte a los menores en una presa fácil de ciberdelincuencia. Si bien hoy en día se ha ido estudiando más este tema, es una problemática que aún debe enfocarse en examinar los métodos preventivos en un panorama mundial.

Según Amo (2016), cabe agregar que, de toda la población. su sector más vulnerable son los menores, porque son quienes más uso les dan a las redes sociales, compartiendo todo tipo de datos personales. Su falta de madurez y su sentido de impunidad por las acciones realizadas a través de Internet (y la creencia de que controlan todo lo relacionado con el mundo online) aumentan la probabilidad de convertirse en víctimas de abusos y delitos en Internet convirtiéndose en un sector digno de mayor protección.

Este es un fenómeno que ha traspasado fronteras. Tanto es así que en España las cifras generan preocupación. Varias entidades como la Sociedad Nacional para la Prevención de la Crueldad contra los Niños- NSCPP- y la Fundación ANAR (Ayuda a Niños y Adolescentes en Riesgo) afirmaron que el *grooming* ha tenido un aumento considerable en los recientes años (300 % para Reino Unido y 400 % para España). Frente a esta situación caótica, es imprescindible tomar medidas al respecto, debido a que, como lo confirmó el Gobierno español en un informe de actuación, es un delito que presenta cifras menores en cuanto a tasas de incidencia reconocida.

En Colombia las cifras de delitos informáticos hacia los menores no son exactas, Según Albert Clemente, profesor de la Universidad de Valencia en su informe "Ciberacoso. Aproximación a un estudio comparado: Latinoamérica y España" "el ciberacoso en Colombia está entre el 40 y el 70% referente a los últimos 11 años" además de un rango de edad entre los 11 y 14 años.

Para concluir, se determina que los menores son los más vulnerables a los delitos en el internet. Sin embargo, se debe enfatizar cada vez más y con mayor frecuencia, en el hecho de que ellos tienen la posibilidad de acceder a artefactos tecnológicos desde una edad temprana, y con esto la entrada a redes sociales con lo que la puerta está abierta a enfrentar varios peligros y riesgos, de igual manera y como se mencionaba anteriormente el sector empresarial también es un atractivo para cometer actos delictivos a través de la red.

Leyes que tipifican actualmente los ciberdelitos en Colombia.

Mirándolo así, la intimidad se constituye como un derecho fundamental e imprescindible, responsable de garantizar la dignidad de las personas en la sociedad. y, asimismo, proteger el cumplimiento de otros, por ejemplo: libertad de expresión, asociación e información. Al ser un derecho tan elemental, este se constituye en el artículo 15 de la Constitución Política, en el cual está consagrado que no podrá promulgarse información de terceros sin una autorización previa.

Teniendo en cuenta el marco normativo se hace necesario definir la delincuencia en las redes sociales la cual se refiere a una serie de fenómenos delictivos, incluida la victimización de diferentes formas de relaciones interpersonales en línea, y traen graves y difíciles consecuencias, principalmente a los menores. La gran dimensión de la tecnológica del abuso hace más fácil la atracción de nuevas víctimas desde diversas acciones: selección de los posibles afectados; atracción y refuerzo del vínculo con la víctima; sexualización, intercambio y difusión de contenidos delicados (incluso retribución económica por la venta de dichas imágenes dentro de la misma red).

No es un secreto que la sociedad actual y la edad tecnológica fomenta implícitamente el delito informativo. No obstante, Colombia no se ha quedado atrás en las medidas impuestas por la Comunidad Económica Europea, quienes se encargaron de difundir acuerdos jurídicos para la protección y disminución de este delito; documentos que se originan del Convenio de Cibercriminalidad (2001); informe que comenzó a hacerse efectivo desde el año 2004.

A nivel internacional se está intentando disminuir esta inclinación delictiva gracias a la nueva tecnología y la ayuda de expertos. Incluso, las vías legales han ayudado a enfrentar este delito. A continuación, se citan algunas de las leyes colombianas que se encontraron en la revisión:

• Ley No. 1273 de 2009

En cuanto a los delitos informáticos su tipificación se da en la Ley 1273 del 2009 que se caracteriza por lo siguiente:

> Complementa el Código Penal y crea la protección de la información, brindando una capa de seguridad jurídica, este texto normativo se divide en dos capítulos; el primero, hace alusión a la vulneración de los derechos contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos, por el otro lado, el segundo capítulo establece los atentados informáticos.

> Esta reglamentación se convirtió en una importante herramienta para las entidades públicas y privadas, dado que con esta se pueden enfrentar con mayor eficacia y eficiencia, los llamados "delitos informáticos", brindando una mayor seguridad a través de las políticas y procedimientos impartidos por el legislador, haciendo uso de este modo, de la jurisdicción penal como medio punitivo para contrarrestar a los infractores de esta reglamentación. (Escobar y Jiménez, 2018, pp. 17-18)

Sin embargo, el problema es el sistema judicial debido a que no es ejecutado de buena forma, a pesar de que la Ley 1273 de 2009, está bien estructurada, tanto así que "fue considerada por el Congreso de la Fiadi (Federación Iberoamericana de Asociaciones de Derecho e Informática) en Santa Cruz de la Sierra" como una de las mejores leyes relacionadas con la detección de crímenes informáticos a nivel del continente. No obstante, en la práctica no se implementa de forma adecuada por parte de los actores judiciales.

Siguiendo con la especificación de la ley, es fundamental afirmar que el primer capítulo se enfoca en colaborar en el trabajo de los auditores de sistemas y, de esta manera, asegurar los requisitos en cuanto a seguridad y eficacia de los datos dentro de las entidades. Claro está, siempre teniendo en cuenta los distintos escenarios de una posible invasión a la información (principal activo dentro de una compañía- ISO/IEC 17799/2005). Por consiguiente, es fundamental proteger los datos confidenciales para no cambiar la estructura interna de la empresa, reduciendo así el riesgo de amenaza.

Tipo penal	Descripción y sanción
269 inciso A "Acceso abusivo a un Sistema informático"	"Aprovechan la vulnerabilidad en el acceso a los sistemas de información o debilidad en la seguridad informática (prisión de 48 a 96 meses, multa de 100 a 1000 SMMLV)".
269 inciso B "Obstaculización ilegitima del sistema de información o red de telecomunicación"	"Bloquean en forma ilegal un sistema o impiden su ingreso a cuentas de correo electrónico financieras y sin el debido consentimiento del titular (prisión de 48 a 96 meses y multa de 100 a 1000 SMMLV)".

269 inciso C “Interceptación ilícita de datos informáticos”	“Obstruyen datos sin autorización legal, en su lugar de origen, en el destino o en el interior de un sistema informático (prisión de 36 a 72 meses”.
269 inciso D “Daños informáticos”	“Cuando una persona que sin estar autorizada modifica, daña o altera, borra o destruye o suprime datos del programa o documentos electrónicos y se hace en los recursos de TIC (Prisión de 48 a 96 meses y multa de 100 a 1000 SMMLV)”.
269 inciso E “Uso de software malicioso”	“Cuando se realice reproducción, adquisición, distribución, se ejecute el envío, o se introduzca o extraiga del país software o programas de computador que produce daño en los recursos TIC (Prisión de 48 a 96 meses y multa de 100 a 1000 SMMLV)”.
269 inciso F “Violación de datos personales”	“El que sin estar facultado sustraiga, venda, envíe, compre, divulgue o emplee datos personales, almacenados en medios magnéticos (Prisión de 48 a 96 meses y multa de 100 a 1000 SMMLV)”.
269 inciso G “Suplantación de sitios web para capturar datos personales”	“Crean una página similar a la de la entidad y envían correos (Spam) como ofertas de empleo solicitan claves de cuentas financieras y hacen traspasos de dinero a terceros (prisión de 45 a 96 meses y multa de 100 a 1000 SMMLV)”.

Tabla 1. Ley 1273 2009 sobre el manejo y la protección de datos

Fuente: (Ojeda-Pérez y Arias-Flórez, 2010, p. 55)

El estado colombiano ha tomado medidas para tratar de reducir los casos de delitos informáticos. Por ejemplo, la ley de 1928 en 2018 volvió a adoptar la Convención sobre Delitos Cibernéticos en un intento de utilizar todos los medios legales para prevenir su desarrollo.

- Ley 1928 del 2018

“Por medio de la cual se aprueba el Convenio sobre la Ciberdelincuencia, adoptado el 23 de noviembre de 2001, en Budapest”.

A partir del año 2009, Colombia tenía un trabajo adelantado en lo que hacía referencia a la defensa de la información y de los datos debido a la ley 1273, sin embargo, en el año 2018 en el que finalizaba el mandato del ahora expresidente Juan Manuel Santos dentro del paquete legislativo fue aprobada la ley 1928 del 24 de julio de 2018.

La ley 1273 del 2009 está más enfocada a la tipificación de los diferentes delitos informáticos, no obstante, en cuanto a la pornografía infantil y demás delitos que atentan contra los menores de edad, no son especificados en la ley, ahora bien, en el año 2018 el presidente de la república en el periodo legislativo Juan Manuel Santos sanciono la ley 1928, donde se incorpora al cuerpo normativo penal, la lucha contra la ciberdelincuencia el convenio aprobado en el año 2001 en Budapest, dicho convenio hace referencia a la luchas contra la ciberdelincuencia, y en ella se hace mayor mención a los delitos que ocurren en el ciberespacio. Cabe aclarar que se convirtió en el primer tratado internacional en la historia sobre ciberdelincuencia.

La consolidación de este acuerdo se basó en la necesidad de evitar las amenazas que pongan en peligro la privacidad y confidencialidad. En resumidas cuentas, se intenta, a partir de una política penal común, establecer lazos cooperativos a nivel internacional para enfrentar de forma conjunta la ciberdelincuencia. Ahora bien, dentro del panorama colombiano también se hace fundamental esta aplicación para tipificar los delitos y, por lo mismo, facilitar su investigación.

En el capítulo II se encuentran regulados los delitos contra los derechos fundamentales antes mencionados, como “la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos”. En este capítulo, el artículo 2 regula la entrada ilegal a los datos personales, que estipula todo el contenido relacionado con la intención de obtener datos personales con fines delictivos, también sobre todo el contenido relacionado con un sistema informático conectado a través de redes. De igual manera se tiene el artículo 3, 4 y 5 hace alusión a la Interceptación ilícita de dispositivos como teléfonos computadores personales, toda forma de filtración de cualquier tipo de información ilegal. Ahora bien, el artículo 6, 7 y 8 hacen referencia a cualquier tipo de abuso, falsificación y fraude informático.

Con respecto a los delitos contenidos en la ley 1928 del 2018 se tiene un componente especial que hace mención de los actos delictivos involucrados con la pornografía infantil, este corresponde al artículo 9 ***“delitos relacionados con la pornografía infantil”***. Cabe aclarar que este concepto alude a todo tipo de material que promueve la pornografía y, asimismo, alude al contenido en el que se evidencia a un menor (sujeto que no ha cumplido 18 años) desde una perspectiva sexual explícita. No obstante, el acuerdo deja la posibilidad de establecer el límite de edad que no puede ser inferior a 16 años. Dentro de sus compromisos, Colombia ha establecido instrumentos legislativos para enfrentar esta problemática.

Tal como ya vimos, el desarrollo normativo en Colombia, parte de la Constitución Política y el ordenamiento jurídico, con las leyes 1273 de 2009 y 1928 de 2018, pero tan bien resulta importante revisar las políticas de orden público del gobierno contra el ciberdelitos, es así, como encontramos la

primera política pública que se desarrolla en torno a los delitos informáticos en Colombia haciendo referencia al CONPES 3701 de 2011 que se titula “Lineamientos de política para Ciberseguridad y Ciberdefensa”. Entre los grandes logros de esta política, destacan las regulaciones y la prevención relacionadas con los delitos informáticos.

Asimismo, se fundamentó el CONPES 3854 de 2016 titulada “Política Nacional de Seguridad Digital de Colombia” (desarrollada hasta el 2020). Entre los esenciales objetivos se destacan los siguientes:

- Establecer un marco institucional preciso alrededor de la seguridad digital, la cual está fundamentada en la gestión de riesgos.
- Implementar los requerimientos pertinentes, con el fin de que los interesados puedan regular su seguridad digital y, por ende, se configure un entorno fiable.
- Considerar la perspectiva de la gestión de riesgos, fortaleciendo la seguridad y el entorno digital para todo el personal relevante a nivel nacional e internacional.
- Reforzar la soberanía nacional y defensa.
- Promover el trabajo conjunto y asistencia en comunidad en temas de seguridad digital desde diferentes panoramas.

En la construcción de estas Políticas Públicas, fueron participes representantes del Gobierno Central, la sociedad en general, el sector privado, la industria de las tecnologías y los académicos, al mismo tiempo de las recomendaciones efectuadas por instancias internacionales. Entre estas organizaciones se encuentran las siguientes entidades: OCDE y la OEA, las discusiones establecidas entre el DNP, MINTIC, el Ministerio de Defensa Nacional y otras asociaciones vinculas con la protección digital en Colombia.

El CONPES 3701/2011 y CONPES 3854/2016, supuso grandes avances del estado colombiano en pro de garantizar tanto la protección de la información de carácter estatal, como la información personal que es trasmitida por millones de usuarios cada minuto, dando la tranquilidad necesaria de no ser interceptada en la red y publicada con fines delictivos.

Contrastar la normativa existente sobre los ciberdelitos en España y Colombia

- Leyes que rigen en España en cuanto a los delitos informáticos.

Según el ordenamiento, los ciberdelitos no están como un tipo penal especial. Sin embargo, el Código penal español si tienen en cuenta diferentes comportamientos ilícitos vinculados con el delito en cuestión. A continuación, se nombran los principales:

- Delitos contra la intimidad

La ley orgánica 10/1995 refiere a los delitos que atentan contra la intimidad, en el artículo 197 se estipula una pena privativa de la libertad de cuatro años, más una multa estipulada a aquellos sujetos que vulneren la intimidad o se apropien de información confidencial sin un debido consentimiento.

En España este tipo de delitos es delicado, debido a la gravedad del hecho, porque se vulnera el derecho a la

privacidad e intimidad. En el apartado 4 del artículo se menciona que:

> “Los hechos definidos en los apartados 1 y 2 del artículo serán penalizados con una sanción de tres a cinco años de prisión, teniendo un agravante cuando: a) Se cometan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros; o b) se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima. Con lo anterior se evidencia el castigo que tendría la persona en caso de incurrir en este tipo de delitos” (Ley Orgánica 10, 1995).

- Delitos informáticos

En el capítulo VI de la ley orgánica 10/1995,código penal español, se regula lo concerniente a las defraudaciones y estafas, el articulo 248 y 264 hacen alusión a los delitos en lo que se utilizan sistemas informáticos con el objetivo de cometer el delito de estafa, inclusive los castigos ascienden a los 5 años de prisión. “Los artículos 255 y 256 mencionan las penas que se impondrán a quienes cometan defraudaciones utilizando, entre otros medios, las telecomunicaciones” (Division Computer Forensic, s.f., párr. 10).

La regulación y sanción de la normatividad española establece estrategias de seguridad informática que buscan reducir la comisión de ciberdelitos, y contribuir a reducir las cifras de víctimas por cuenta de estos.

- Delitos relacionados con el contenido

Por otro lado, en el artículo 186 del Código Penal español, se fijan las condenas que deberán asumir aquellos que promuevan y difundan contenido pornográfico dentro del círculo de menores de edad o personas incapaces. En relación con lo anterior, en el artículo 189 se describen los correctivos y penas a quien produzca y difunda material sexual en el que hayan participado menores de edad. Asimismo, se establece en esa normativa el tipo de privación de la libertad que deberán asumir los delincuentes.

- Delitos relacionados con la infracción de la propiedad intelectual y derechos conexos

El Artículo 270 de la ley orgánica N ° 10/1995 del código en cuestión alude a la propiedad intelectual, es decir, creaciones de diversos tipos que sean promovidas sin el debido consentimiento. Igualmente, en el artículo 273 se tiene en cuenta a las patentes que son difundidas e introducidas sin la autorización del titular. Todo lo anterior con el fin de asegurar la propiedad intelectual y detener el plagio.

- Convenio de Budapest

La Convención sobre la Ciberdelincuencia o la Convención de Budapest es el único tratado multilateral vinculante destinado a combatir la ciberdelincuencia. Fue redactado por el Consejo Europeo en 2001 con la participación de países observadores. La Convención proporciona un marco para la cooperación entre las partes del tratado. Está abierto para ratificación incluso a Estados que no son miembros de la Consejo Europeo. El Convenio de Budapest prevé (i) la criminalización de la conducta, que va desde ilegal acceso, datos e interferencia de sistemas al fraude informático y la pornografía

infantil. (en materia procesal y las herramientas legales para realizar la investigación del ciberdelito y la obtención de pruebas electrónicas y evidencias que contribuyan a identificar la responsabilidad de la comisión del ciberdelito) (iii) policía internacional y cooperación judicial en materia de ciberdelito y pruebas (Council of Europe, 2001).

Existen ciertas similitudes al momento de comparar la aplicación del convenio tanto en España y Colombia, por ejemplo, algunos artículos en los que de manera similar se establecen procedimientos que hacen referencia a interceptaciones, acceso abusivo, violación de datos entre otros, de la misma forma entre Colombia y España.

En Colombia, la Ley N ° 1273 de 2009 que modificó el Código Penal colombiano con lo que, de este modo, se estableció un nuevo bien jurídico tutelado. Este fue titulado "de la protección de la información y de los datos". Al respecto, es necesario afirmar que se preservan integralmente los sistemas, los cuales utilizan las tecnologías de la información y las comunicaciones, entre otras medidas. Por otra parte, en España el tema es abordado en el Código Penal de 1995 aprobado por Ley-Orgánica 10/1995, donde son regulados los delitos informáticos. Es decir que en España existe un solo compendio que regula los delitos informáticos mientras que en Colombia existe un capítulo que regula estas disposiciones, una ley específica para la regulación y sanción de los ciberdelitos.

Respecto a delitos específicos como lo es la pornografía infantil, España como ya se hizo mención, cuenta la ley orgánica 10/1995 del código penal más específicamente con el artículo 189 de este, el cual hace referencia al tratamiento que se le da en ese país, por su parte Colombia, cuenta con la ley 1928 del 2018 la cual hace más énfasis con respecto a los ciberdelitos, destacando un ítem sobre los delitos relacionados con la pornografía infantil.

Derechos fundamentales vulnerados

Como bien se mencionó en los anteriores apartados estos crímenes realizados bajo estas plataformas tecnológicas, vulneran los derechos de las víctimas, pero ¿cuáles derechos fundamentales se vulneran en específico?

Tanto en Colombia como España "han reconocido y ratificado la declaración universal de los derechos humanos, la cual fue proclamada por la Asamblea general de las naciones unidas en parís en el año de 1948".

Como se estableció anteriormente, los delitos más generales en esta modalidad de ciberdelincuencia son el ciberbullyng, la violación a la intimidad, la pornografía infantil, la estafa, el hurto informático, los cuales vulneran derechos fundamentales, y algunos de ellos son:

- **Derecho a la intimidad:**

El artículo 12 de la declaración universal de derechos humanos, expresa que ninguna persona puede obstaculizar las esferas sociales de otro sujeto. Además, cualquiera tiene derecho a protegerse desde la vía legal contra las agresiones cometidas a su intimidad.

A su vez, el art 15 Constitución Nacional, afirma que todos tenemos derecho a la privacidad personal y familiar, y a la preservación del buen nombre y "el

Estado debe respetarlos y hacerlos respetar" (Asamblea Nacional Constituyente, 1991, art. 15).

Es claro, que este derecho se ve gravemente vulnerado en varios ciberdelitos, por ejemplo, en el momento en el que se dejan al descubierto datos que son privados.

Se puede presentar también en el ciberbullyng ya que en este puede causar un daño considerable a la reputación y al buen nombre de la persona.

Y lo mismo pasa en el sexting o en la pornografía, toda vez que inescrupulosos hagan pública información sin consentimiento de las personas o la utilicen con fines delictivos.

- **Derecho a la no discriminación:**

Sobre este derecho, el artículo 2 de la declaración universal de los derechos humanos regula básicamente "la no discriminación ya sea por la raza, sexo, religión, opinión política y cualquier otra condición".

El artículo 13 de la Constitución Política, sobre este mismo derecho expresa: "todas las personas nacen libres e iguales ante la ley y recibirán la misma protección y trato por parte de las autoridades, y gozarán de los mismos derechos, libertades y oportunidades, no basadas en género, raza, etnia u origen familiar, idioma, religión, opinión o cualquier otra discriminación" (Asamblea Nacional Constituyente, 1991, art. 13).

Este derecho es vulnerado más que nada, mediante la figura del ciberbullyng, ya que mediante estas se observa cómo se realizan burlas de condiciones físicas y psicológicas a través de medios tecnológicos, evidenciándose una clara manifestación de discriminación hacia la víctima.

- **Derecho a la Libertad sexual:**

Está estipulado en el artículo primero de la Declaración de los Derechos) Sexuales" (Declaración del XIII Congreso Mundial de Sexología celebrado en Valencia, España en 1997)

En Colombia, este derecho está resguardado en la sentencia T-732 de 2009, la Corte Constitucional, declara que todos los sujetos poseen el derecho a elegir sobre su propio cuerpo. Asimismo, tienen la posibilidad de elegir con quién desean hacer su encuentro. En resumidas cuentas, la Constitución fija las bases para que no exista ningún tipo de violencia que afecte a otra persona (discriminación, prostitución forzada, abuso).

- **Derechos de los niños:**

Consagrado en el artículo 44 de la Constitución Política: "Son derechos de los niños: la vida, la integridad física, la salud, la seguridad social, la alimentación equilibrada, su nombre y nacionalidad, tener una familia y no ser separados de ella, el cuidado, el amor, la educación, la cultura, la recreación, la libre expresión de su opinión y como tal es obligación del Estado velar por la protección de dicho derechos" (Asamblea Nacional Constituyente, 1991, art. 44).

Cabe mencionar este derecho ya que como en un apartado anterior se mencionó, esta es una de las poblaciones más afectadas en esta forma de delitos, por ende, es uno de los derechos más vulnerados.

- **Derecho al Olvido:**

Este se refiere básicamente a que la persona tiene el derecho a que se le elimine sus datos personales que estén subidos a internet, ya sea porque ya no

son útiles, porque ya no se tenga el consentimiento o porque son de origen ilegal. Con esto también se puede solicitar el bloqueo de los links que lleven a la información de esto.

En España existe una sentencia que abarca de manera importante este derecho la STJUE de Google contra Mario Costeja y la Agencia Española de Protección de Datos (AEPD), la cual marca un ítem importante a nivel jurisprudencial del derecho al olvido, describe básicamente que el problema de este derecho se relaciona básicamente con el contenido que es publicado por el editor en Internet, que cuando es indexado por un motor de búsqueda (es decir cuando se realiza la aparición en los resultados de búsqueda de los buscadores) se difunde ampliamente y afecta negativamente a la víctima. Cabe aclarar que el motor de búsqueda es una persona jurídica cuyo fin es clasificar ordenadamente los contenidos de internet y con esto darles visualización a los usuarios.

También abarca un tema importante el cual es la responsabilidad de los motores de búsqueda en la vulneración de este derecho, por un lado, se dice que estos pueden ubicar, almacenar, organizar y presentar datos, por lo que tiene la decisión de la finalidad y uso del tratamiento de estos, lo que los considera como responsables, además de que mediante estos buscadores se tienen unos efectos considerables en la difusión de la información. Otra parte y por el contrario defiende a estos buscadores argumentando que ellos no definen los datos personales como tales si no como información que da internet, además de que el buscador solamente facilita la búsqueda por lo cual no tiene responsabilidad alguna.

Básicamente la decisión del Tribunal de Justicia de la Unión Europea planteo jurisprudencia que ayuda en la resolución de litigios y junto con esto dejo responsabilidad a los motores de búsqueda para que procuren realizar la eliminación de los datos que se requieran.

En Colombia este derecho no está regulado en específico, En la Sentencia T-098/17 de la Corte Constitucional se hace mención del derecho al olvido de la información negativa, pero hace es alusión a la información que dan los medios de comunicación, acerca de una persona, y del derecho que tiene a que se rectifique esta información que pudo llegar haber dañado su buen nombre.

Lo más cercano al derecho al olvido en Colombia es el Habeas Data, regulado en la Ley estatutaria 1266 de 2008 la cual tiene como planteamiento darles el derecho a las personas de ‘’conocer, actualizar y rectificar las informaciones que estén almacenadas en bancos de datos, específicamente los datos financiaron, crediticios y comerciales’’.

En donde también se estipula el Habeas Data es en la Ley 1581 de 2012 y el Decreto 1377 de 2013 en donde se habla de la protección de datos personales, en estas normas se establece como derecho constitucional de todos los ciudadanos comprender, actualizar y corregir toda muestra de datos personales almacenados o recibidos en tratamiento básico en entidades públicas y privadas. En base a esta Ley 1581 de

2012 y de acuerdo con las disposiciones de la Ley Nacional 1581, se estableció el Registro Nacional de Bases de Datos (RNBD), el cual es un catálogo público que contiene información personal en bases de datos en diferentes entidades.

La Corte Constitucional Colombiana en la Sentencia T-176A/14 expone que el derecho de Habeas Data es un derecho fundamental que permite autorizar, incluir, certificar y suprimir información personal de las bases de datos.

Aunque existan estas normativas en Colombia, que dan el derecho a la victima de rectificar, agregar o suprimir, información personal de bases de datos, se presenta un vacío jurídico en cuanto a la protección del derecho al olvido, el cual es importante para la reparación de las víctimas de los delitos informáticos.

Metodología

En esta investigación se eligió utilizar la investigación cualitativa, la cual atraviesa varias etapas en su desarrollo uno de ellos es la recolección productiva de datos, a partir de estos y secuencialmente se establecen otras etapas como el análisis de estos , es decir que partiendo del problema es necesario establecer que información relevante aporta el problema de investigación , se analizan estos datos para poder luego hacer una entrada al campo que no es más que observar e identificar otros rasgos que no fueron definidos en la recogida de datos y que resultan más sensibles a la observación para finalmente analizar cada uno de estos datos suministrados y hacer difusión de estos (Rodríguez-Gómez et al, 1996).

De igual manera se utilizará el método inductivo, como lo expresa (de Rueda, 1997), quien configuró esta herramienta investigativa con las siguientes características: puede ser parcial o completa; el razonamiento que se deduce puede establecerse de situaciones específicas a conocimientos generales; alude directamente a todo el proceso e instrumento utilizados en el transcurso de la investigación.

Sumado al anterior concepto, se empleará el análisis de contenido entendido como una agrupación de herramientas metodológicas, las cuales se implementan a los discursos (contenidos) diversificados. Es decir, hay que aclarar que se trata de una hermenéutica basada en la deducción, es decir, basada en la inferencia (Bardin, 1986). Sin duda, es una técnica cualitativa para el análisis, además de la lectura y la hermenéutica.

Conclusiones

Debido al surgimiento de nuevas tecnologías, los ciberdelincuentes han buscado la manera de delinquir en redes sociales y en todas las plataformas informáticas, valiéndose de cualquier medio con fines delictivos, frente a la ventaja que tiene cada persona de contar con un dispositivo electrónico, existe el riesgo de que se pueda materializar un delito, no obstante los ciberdelitos están más sesgados hacia los menores de edad, debido a la vulnerabilidad a los que estos se encuentran expuestos.

Colombia cuenta con la normatividad suficiente en materia preventiva y sancionatoria frente a la comisión de delitos informáticos, empezando con la Constitución Política de 1991 la cual es

garante de los derechos fundamentales vulnerados a causa de estos delitos además de la Ley No. 1273 de 2009, en la que se tipificaron los ciberdelitos, complementado el Código Penal, sin embargo, es necesario establecer los mecanismos de control para la vigilancia y la aplicabilidad del marco legal.

Ahora bien, Colombia y España se encuentran suscritas al convenio del Budapest razón por la cual la normatividad regula los mismos preceptos; no obstante, en ambos países se pretende buscar la manera de mejorar estas leyes, las cuales deben ir mancomunadamente con el desarrollo de las tecnologías, debido a las nuevas metodologías de ataque que implementan los ciberdelincuentes.

Identificados los derechos fundamentales más vulnerados por los ciberdelitos se pueden señalar la discriminación, la libertad sexual, la protección especial a los niños, el derecho a la intimidad y el derecho al olvido, frente a la identificación de las conductas que tipifican delitos plenamente regulados en nuestro código penal, es necesario establecer los correctivos necesarios para las sanciones de las conductas cometidas y la prevención frente a la comisión de más conductas que aún son atípicas ya que a diario los ciberdelincuentes tienen la oportunidad de violar estos derechos debido al crecimiento tecnológico.

Referencias bibliográficas

Amo, A. (2016). *El acceso de los menores de edad a las redes sociales.* Universidad de Salamanca. https://gredos.usal.es/bitstream/handle/10366/131719/TG_AmoAlonso_Acceso.pdf;jsessionid=73CF0E72EEDA4D537E0A80C52AB2DA83?sequence=1

Asamblea Nacional Constituyente. (1991). Constitución Política de 1991. Gaceta Constitucional N°. 116 del 20 de julio de 1991. Bogotá, D.C., Colombia.

Bardin, L. (1986). *El análisis de contenido.* Akal.

Centro Cibernéutico Policial. (2017). *Amenazas del cibercrimen en Colombia 2016-2017.* Comando de Atención Inmediata [CAI]. https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

Congreso de la República de Colombia. (2009). Ley 1273 del 5 de enero de 2009. Diario Oficial No. 47.223. [Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los...]. Bogotá,D.C., Colombia.

Congreso de la República de Colombia. (2018). Ley 1928 del 24 de julio de 2018. Diario Oficial No. 50.664. [Por medio de la cual se aprueba el “Convenio sobre la Ciberdelincuencia”, adoptado el 23 de noviembre de 2001, en Budapest]. Bogotá,D.C., Colombia.

Congreso de los Diputados. (1995). Ley Orgánica 10 del 23 de noviembre de 1995. Boletín oficial del Estado A-1995-25444. Madrid, España.

Consejo Nacional de Política Económica y Social. (2011). *Conpes 3701 de 2011. Lineamientos de política para la Ciberseguridad y Ciberdefensa.* https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

Council of Europe. (2001). *Convention on Cybercrime.* Council de L'Europe. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

de Rueda, S. (1997). *Conceptos básicos de investigación.* https://investigar1.files.wordpress.com/2010/05/conceptos.pdf

Division Computer Forensic. (s.f.). *Legislación .* Delitos informáticos: https://www.delitosinformaticos.info/delitos_informaticos/legislacion.html

Escobar, D., & Jiménez, L. (2018). *Eficacia de las normas penales colombianas para prevenir y sancionar los ciberdelitos.* Universidad de Ibagué. https://repositorio.unibague.edu.co/jspui/bitstream/20.500.12313/1925/1/Trabajo%20de%20grado.pdf

Gorostidi, L. (2020). La pluralidad de víctimas derivada de la elevada lesividad en los ciberdelitos: una respuesta penal proporcional. *Estudios de Deusto, 68*(1). doi:10.18543/ed-68(1)-2020pp201-221

Interpol. (2020). *Ciberdelincuencia: efectos de la COVID-19.* Secretaría General de Interpol. https://www.interpol.int/es/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-Design_02_SP.pdf

Ojeda-Pérez, J., & Arias-Flórez, M. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. *Cuadernos de Contabilidad, 11*(28), 41-66. http://revistas.javeriana.edu.co/index.php/cuacont/article/view/3176/2416

Pons, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. *Revista Latinoamericana de Estudios de Seguridad*(20), 80-93. https://revistas.flacsoandes.edu.ec/urvio/article/view/2563/1608

Rodríguez-Gómez, G., Gil-Flores, J., & García-Jiménez, E. (1996). *Metodología de la investigación cualitativa.* Ediciones Aljibe. https://www.researchgate.net/publication/44376485_Metodologia_de_la_investigacion_cualitativa_Gregorio_Rodriguez_Gomez_Javier_Gil_Flores_Eduardo_Garcia_Jimenez

Ruiz, J. (2016). *Ciberamenazas: ¿el terrorismo del futuro?* Institución Español de Estudios Estratégicos . http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO86-2016_Ciberamenazas_JRuizDiaz.pdf

TicTac. (2019). *Tendencias del Cibercrimen en Colombia 2019-2020.* Cámara Colombiana de Informática y Telecomunicaciones. https://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

Torres-González, D. (2015). La información y la comunicación del riesgo de origen tecnológico en la empresa Puerto Moa. *Ciencia & Futuro, 5*(1), 104-122. https://revista.ismm.edu.cu/index.php/revista_estudiantil/article/view/1031/537

Martinez, Otero- Juan, M (2016). La aplicación del derecho al olvido en España tras la STJUE Google contra AEPD y Mario Costeja http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2070-81572017000100004&lng=es&nrm=iso