LA NATURALEZA JURÍDICA DE LOS DELITOS INFORMÁTICOS EN COLOMBIA

MARÍA PAULA GUARNIZO PORTELA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
IBAGUÉ
2020

LA NATURALEZA JURÍDICA DE LOS DELITOS INFORMÁTICOS EN COLOMBIA

MARÍA PAULA GUARNIZO PORTELA

Monografía como trabajo de grado para optar por el título de
Especialista en Seguridad Informática

Director:
ALEXANDER LARRAHONDO NUÑEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
2020

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

_____

Firma Presidente del Jurado

_____

Firma Jurado

_____

Firma Jurado

Ibagué, junio 4 de 2021

DEDICATORIA

Esta monografía está dedicada a mi madre, quien me apoyo de manera incondicional durante toda la especialización.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

GLOSARIO

ANTIJURIDICIDAD: Conocido como el desvalor que ostenta un hecho típico inverso al ordenamiento jurídico. La antijuridicidad es lo contrario al Derecho.

ATAQUE: Es el aprovechamiento de una o varias vulnerabilidades, en las cuales se emplea una técnica de ataque con el objetivo de devastar, exhibir, perturbar o invalidar desde un sistema de información o ya sea la información que el sistema manipula.

BIEN JURÍDICO: en el Derecho Penal puede definirse como todo bien, situación o relación deseados y protegidos por el Derecho para mantener el orden social

BIENES JURÍDICOS INTERMEDIOS: Son aquéllos cuya tutela va dirigida a evitar la lesión mediata o inmediata de otros bienes jurídicos

CIBERATAQUE: Es la gestión efectuada en el ciberespacio que implica la disponibilidad, confidencialidad e integridad de la información, por medio del acceso no autorizado, la alteración, adulación o pérdida de los sistemas de información y telecomunicaciones o las infraestructuras que los soportan.

CIBERDELITOS: Es una acción delictiva o abusiva donde son objeto los computadores y las diferentes redes de comunicaciones, en donde se pueden utilizar el computador como instrumento del delito, o de igual manera puede ser el objetivo un sistema informático o la información contenida en él.

CÓDIGO MALICIOSO: Software capaz de realizar un proceso no autorizado sobre un sistema con un deliberado propósito de ser perjudicial.

CONDUCTA DOLOSA: Cuando el agente comete una infracción penal conociendo los hechos y sus consecuencias.

CONDUCTA PUNIBLE: Es aquella que, por sus características, puede o debe recibir una punición (castigo o pena)

DELITO: Acción típica, antijurídica, imputable, culpable, sometida a una sanción penal y a veces a condiciones objetivas de punibilidad.

DELITO INFORMÁTICO: Un delito cibernético, es un crimen centrado en el ser humano… que dañan la intimidad o el patrimonio económico y de forma colateral a los sistemas de información

DENEGACIÓN DE SERVICIO: Es la actividad encausada en inundar con sinnúmero peticiones de servicio a un servidor, hasta que este no logra dar abasto con todas y siendo esta la manera de incitar su colapso.

IMPUTAR: Atribuir la responsabilidad de un delito a una persona.

LEGISLADOR: Se refiere a quien hace, establece o da las leyes para la ordenación de la sociedad.

ORDENAMIENTO JURÍDICO: Es el conjunto de normas jurídicas que rigen en un lugar determinado en una época concreta.

PUNIBLE: Es toda conducta que va contra la Ley. Se dice que una acción es punible cuando se considera que merece ser castigada legalmente.

SEGURIDAD DE LA INFORMACIÓN: Son varios aspectos que hacen parte de la seguridad de la información como lo es la conservación de la reserva, integridad y la acción de la información. Integrando entre otras propiedades, como lo es la legitimidad, compromiso, confabulación y prevención del repudio.

TIPICIDAD: La tipicidad es el encuadramiento de una conducta humana en un tipo penal, el cual busca proteger el bien jurídico tutelado por el legislador.

TIPO PENAL: Se entiende por la representación exacta de las acciones u omisiones las cuales se encuentran establecidas como delito y a las que se les estipula una pena o sanción.

VACÍO JURÍDICO: También denominada laguna jurídica o del Derecho o limbo jurídico (también llamado vacío legal) es la ausencia de reglamentación legislativa en una materia concreta.

VIRUS: Segmento de código que puede copiarse, tras la satisfacción de alguna condición lógica o temporal, para infectar otros programas, a los que ataca modificándolos, destruyéndolos, etc.

VULNERABILIDAD: Es la extenuación o inexactitud en el control que da pie a que una amenaza ejerciese contra un objetivo o recurso del sistema al cual va dirigido el ataque.

RESUMEN

La aplicación en el sistema jurídico de la Ley 1273 de 2009, Artículo 269 del código Penal, ha marcado un hito en la legislación colombiana, porque ampara un bien jurídico no mencionado antes en las leyes y que tiene que ver con la protección de la información y de los datos; de la misma forma, consiente en tipificar y penalizar los delitos cometidos contra este bien jurídico. Sin embargo, tras el avance en las tecnologías de la información y las comunicaciones, también se avanza en las nuevas formas de delinquir; es así, como faltas conocidas como "delitos tradicionales" ahora se ejecutan con ayuda de medios tecnológicos o mediante la utilización de estos, sin que exista una penalización expresa en el ordenamiento jurídico existente.

Para la identificación de los delitos cometidos mediante o a través de medios informáticos, se realizó inicialmente un recorrido por la normatividad colombiana, respecto a la comisión de delitos por medios informáticos, partiendo del Decreto 1360 de 1989; que reglamenta la inscripción del Soporte Lógico (software) en el Registro Nacional del Derecho de Autor; hasta el Documento CONPES 3854 de 2016, que pretende diseñar una política pública de seguridad informática, el análisis de esta normativa permitió identificar algunos vacíos que tiene la ley frente a la comisión de estos delitos y de cara a la realidad se revisó como usualmente delitos tradicionales que se hayan cometido mediante el uso de medios electrónicos, pretenden ser tipificados como delitos informáticos.

Se realizó también, una investigación de los delitos informáticos más comunes en Colombia, basada en los informes de la Seguridad Informática e Investigación Forense de entidades como investigadores del Centro de Capacidades para la Ciberseguridad de Colombia (C4) de la Policía Nacional, del Tanque de Análisis y creatividad de las TIC (TicTac), y la Cámara Colombiana de Informática y Telecomunicaciones (CCIT), donde se determinó que en el 2019, en el país los incidentes cibernéticos se incrementaron en un 54% con respecto al 2018. Igualmente, de los 28.827 casos reportados, solamente el 55.4% (15.948) de los casos, se tipificaron como contravenciones a la Ley 1273 de 2009 y solamente se

lograron realizar 274 capturas por la infracción de esta norma[1]. Es así como, el 44.6%, de los incidentes informáticos denunciados no fueron tipificados como delitos a la luz del artículo 269 del CPC; pero si afectaron en su bienestar personal, social, económico y político a ciudadanos y empresas del país. Por esta razón, en el documento se propuso una metodología sencilla, para que los profesionales no abogados puedan identificar fácilmente los delitos informáticos de acuerdo con lo reglado en el Código Penal Colombiano.

[1] El Tiempo, En el 2019 se reportaron más de 28.000 ciberataques en Colombia, [en línea] 2019 [consultado 15 de mayo de 2020]. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-ecnologia/reporte-de-ciberataques-en-colombia-2019-de-policia-nacional-y-ccit-428790

INTRODUCCIÓN

Las organizaciones actuales requieren para su funcionamiento de una variada, amplia y compleja apropiación de sistemas de información, que unido a la dinámica de cambio de las diferentes tecnologías de la información y las comunicaciones, generando en éstas, compuestas representaciones de fusiones que han permitido ampliar los mercados, acercando el mundo. Estos cambios, de igual manera como han traído a las personas e instituciones también ha generado al mismo tiempo amenazas, riesgos y espectros de incertidumbre.

Paralelamente, con el avance de las tecnologías el Derecho también se ha visto obligado a repensar o incluso a replantear aquellas categorías dogmáticas tradicionales. La teoría científica del delito, en los últimos 150 años se ha basado en la causal objetiva - subjetiva, es así como, aparecen en el medio exterior conductas comúnmente denominadas delitos tradicionales (el hurto, la tentativa de homicidio, etc). A finales del siglo XX surgen nuevas categorías en la teoría del delito que permiten precisar la imputación legal y aclaran el alcance del nexo de causalidad, denominada imputación-objetiva[2], que ha permitido anticiparse a la protección de objetos ideales e inmateriales, como es el caso de la propiedad intelectual (derechos morales de autor art. 270-2 CPC.) e industrial. Surge entonces, un nuevo paradigma delictivo en una sociedad modificada digitalmente y que requiere de la protección de los tres pilares (Confidencialidad, integridad y disponibilidad) de un bien denominado *información.* Lo particular de estas conductas punibles, es que no tienen un *lugar* de ocurrencia; esto sucede en un ámbito deslocalizado llamado ciberespacio o la Web.

Con la aparición de nuevas modalidades criminales como el Cibercrimen y los delitos informáticos, colocan a la doctrina contemporánea frente a diferentes modos

[2] CATRO MUÑOZ, Juan José, La imputación Objetiva [en Línea] 2016, [consultado 25 de agosto de 2020]. Disponible en: https://www.asuntoslegales.com.co/analisis/juan-jose-castro-munoz-530496/la-imputacion-objetiva-2444266

del delito y la pena, para lo cual se hace necesario tener en cuenta que: en primer lugar, la noción del delito es compleja pues este no se ejecuta en un medio físico se realiza en un lugar indeterminado llamado ciberespacio, los medios de ejecución son técnicas especializadas y se busca la protección de un bien completamente inmaterial. En segundo lugar, estos delitos son cometidos en una sociedad digitalmente modificada, que funciona en torno a la información, que se caracteriza por el incremento de un contexto social de hiperconexión digital, donde se necesita proteger la información y los datos como un bien jurídico de naturaleza intermedia, y este a su vez protege otros derechos constitucionales y bienes jurídicos como la intimidad personal, el patrimonio económico, y la autodeterminación informática[3]. Y en tercer lugar, cuando se desarrollaron las teorías del crimen se estaba pensando en un medio físico, jamás en el ciberespacio.

Partiendo del análisis anterior, la monografía tiene como propósito establecer si el ordenamiento jurídico existente en Colombia, contiene los elementos normativos necesarios para penalizar las conductas inadecuadas asociadas con delitos informáticos. Para lograr este objetivo se requiere primero hacer una revisión a la normatividad vigente en Colombia, frente a la identificación, tipificación y penalización de los delitos informáticos; como segunda medida, identificar los delitos informáticos que presentan mayor ocurrencia en Colombia; posteriormente identificar conductas dolosas inapropiadas cometidas mediante el uso de sistemas y/o medios electrónicos, no tipificados en la Ley como delitos informáticos y proponer un procedimiento para la definición de un delito informático y que pueda ser aplicado por profesionales no abogados.

[3] POSADA MAYA, Ricardo, Una Aproximación a la Criminalidad informática en Colombia, 2017. en Revista de Nuevo Foro Penal No. 88, enero-junio 2017, Universidad EAFIT

1. DEFINICIÓN DEL PROBLEMA

El documento CONPES 3701 de 2011 expone que:

> …el uso de las tecnologías de la información y las comunicaciones trae consigo cambios y retos permanentes y se constituye como uno de los pilares del mundo globalizado. De manera simultánea el avance de estas tecnologías ha incrementado el uso de medios tecnológicos con fines delictivos alrededor del mundo. La continua evolución, crecimiento y sofisticación de los ataques cibernéticos, al igual que la convergencia tecnológica, ponen de manifiesto la necesidad de adoptar las medidas y controles que permitan proteger al Estado ante estas nuevas amenazas. El aumento de la capacidad delincuencial en el ciberespacio, así como la utilización de nuevas tecnologías para generar amenazas informáticas, constituyen una preocupación común a todos los países, dado que impactan de manera significativa la seguridad de la información, en los ámbitos tanto público como privado e incluyendo a la sociedad civil[4].

Los cambios generados por los avances informáticos, especialmente por la internet han afectado la forma como se relacionan las personas, las empresas y el Estado, se han disminuido notoriamente los tiempos de realización de actividades y transacciones, se han acortado las distancias con el mundo y la información fluye con rapidez; otra gran ventaja es la facilidad con la que se pueden entablar relaciones sociales y comerciales.

De la misma manera, como los medios informáticos generan grandes beneficios, conllevan también a soportar altos riesgos; se evidencia la comisión de una serie de actos con consecuencias jurídicas, a través del uso de la tecnología informática y de las telecomunicaciones, que afectan de manera directa los bienes jurídicos protegidos por el Legislador quien es la persona u órgano del cual provienen las leyes. Un bien jurídico se define como todo bien, situación o relación deseados y

[4] DEPARTAMENTO NACIONAL DE PLANEACIÓN -DNP. Documento CONPES 3701 de 2011 [en línea] 2011. [consultado 15 de mayo de 2020]. Disponible en: https://www.mintic.gov..co /portal/604/articles-3510_documento.pdf

protegidos por el Derecho para mantener el orden social,[5] estos pueden ser individuales o colectivos; materiales e inmateriales de las personas o de las cosas. El bien jurídico es un concepto importante dentro las ciencias penales; la afectación de un bien jurídico cimienta bases para el establecimiento de un castigo punitivo a las conductas que lo lesionan o lo ponen en peligro y constituye un requisito ineludible para el ejercicio del *ius puniendi*[6] que es la facultad sancionatoria que tiene el Estado y se traduce literalmente como derecho a penar o derecho a sancionar.

Aparecen entonces tres tipos de delitos, que usualmente llegan a ser confundidos y tergiversadas sus definiciones generalmente denominados como "delitos informáticos": los primeros son aquellos delitos tradicionales cometidos a través de computadoras o de la internet (v.gr. difusión de pornografía infantil o extorsión entre otros), los segundos son las conductas dolosas cometidas "contra" sistemas informáticos y que inciden directamente sobre el *software*, soporte lógico o programas que permiten el procesamiento de datos e información (v.gr. espionaje informático, sabotaje entre otros) y el tercer tipo de delito son aquellos que se cometen contra el *hardware* o soporte físico de un sistema informático, o sea la parte material de una computadora, estos delitos pueden ser denominados, en términos generales como delitos patrimoniales, de la categoría de daños.

En el presente documento se analizarán inicialmente los delitos cometidos contra el software, soporte lógico o programas, definidos por la Ley 1273 de 2009 o "ley de delitos informáticos", donde se contempla como bien jurídico intermedio tutelado por el legislador, la protección de la información y los datos, allí mismo se tipifican nueve tipos penales orientados a la protección de la información, los datos y el patrimonio económico. Estos delitos pueden ser agrupados en tres tipos diferentes o ejes sobre los cuales se estructuran: los primeros son los cometidos con el fin de destruir o inutilizar la información, datos o programas informáticos, directamente ligados con el sabotaje de información; los segundos son los que se cometen mediante el acceso indebido a sistemas de información vinculados con el espionaje informático y los terceros son los que implican manipulación o alteración de datos y son los ligados con fraude informático.

Posteriormente, serán tratados otros delitos cometidos mediante sistemas informáticos de los denominados "delitos tradicionales" como la extorsión, difusión

[5] EL BIEN JURÍDICO EN EL DERECHO PENAL, [en línea] 2018. [consultado el 15 de mayo de 2020]. Disponible en: https://www.palladinopellonabogados.com/el-bien-juridico-en-el-derecho-penal/

[6] MAYER LUX, Laura; EL BIEN JURÍDICO PROTEGIDO EN LOS DELITOS INFORMÁTICOS, [en línea] 2017 [consultado el 15 de mayo de 2020]. Disponible en: https://scielo.conicyt.cl /scielo.php?script= sci_arttext&pid=S0718-34372017000100011

de pornografía infantil, entre otros, la forma como deben ser abordados por los jueces al momento de aplicar la Ley.

1.1 ANTECEDENTES

En el compendio hecho por Ojeda y Rincón con respecto a los Delitos informáticos y el entorno jurídico vigente en Colombia, se establece que la Ley 1273 del 5 de enero de 2009, reconocida como la Ley de Delitos Informáticos, sus antecedentes jurídicos se remontan veintiún años atrás, con el Decreto 1360 de 1989 el cual reglamenta la inscripción del soporte lógico (software) en el Registro Nacional de Derecho de Autor, que sirvió como elemento normativo para solucionar los requerimientos presentados por los desarrolladores de software, que buscaban la protección a la propiedad intelectual de los creadores de soluciones informáticas y aplicativos.

Posteriormente, en 1993 la Ley 44, capítulo IV en los artículos 51 y 52, describe conductas delictivas contra los Derechos de Autor, que conjuntamente con el Decreto 1360 de 1989, amparan y reglamentan la inscripción del Soporte Lógico en el Registro Nacional de Derechos de Autor, teniendo en cuenta que el software es considerado un elemento informático. Estas normas sirvieron como base para poder penalizar y sancionar algunas violaciones a los Derechos de Autor que motivaron en parte la reforma del Código Penal Colombiano (Ley 599 de 2000) quedando de la siguiente manera: en el Capítulo Único del Título VII, se determinan los Delitos contra los Derechos de Autor, así: Artículo 270: Violación a los derechos morales de autor. Artículo 271: Defraudación a los derechos patrimoniales de autor. Artículo 272: Violación a los mecanismos de protección de los derechos patrimoniales de autor y otras defraudaciones.[7]

En el Código Penal Colombiano, existen otros delitos tipificados, que pueden ser tenidos en cuenta al momento de penalizar un delito informático, en el Capítulo séptimo del Libro segundo, del Título III: Delitos contra la libertad individual y otras garantías, trata sobre la violación a la intimidad, reserva e interceptación de comunicaciones: allí podemos encontrar los siguientes delitos, que aunque no definidos como delitos informáticos, pueden ser tenidos en cuenta para tal fin estos son: Artículo 192: Violación ilícita de comunicaciones. Artículo 193: Ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Artículo 194: Divulgación y empleo de documentos reservados. Artículo

[7] OSORIO MORENO, César Alejandro. Evolución de la protección penal del Derecho de Autor en Colombia. [en línea]. 2010 [consultado en noviembre 1º. de 2020]. Disponible en: http://www.scielo.org.co/ scielo.php?script =sci_arttext&pid=S0121-86972010000200007

195: Acceso abusivo a un sistema informático. Artículo 196: Violación ilícita de comunicaciones o correspondencia de carácter oficial. Artículo 197: Utilización ilícita de equipos transmisores o receptores. Estos artículos son concordantes con el artículo 357: Daño en obras o elementos de los servicios de comunicaciones, energía y combustibles.[8]

En el 2001 la Ley 679, instauró el Estatuto para evitar y contrarrestar delitos como la explotación, la pornografía y el turismo sexual con niños menores de edad, igualmente instaura prohibiciones para los proveedores o servidores, administradores o usuarios de redes sociales, frente a alojar imágenes, textos, documentos o archivos audiovisuales que exploten a los menores en actitudes sexuales o pornográficas. Esta Ley impone sanciones administrativas, es decir solo prohibiciones, y deja un vacío jurídico ya que no contiene sanciones penales, si se tiene en cuenta que estas conductas son tal vez de las más frecuentes y pueden ser considerados como verdaderos delitos informáticos.

El Estado en su lucha por proteger a los niños, niñas y adolescentes, sancionó la Ley 1336 del 21 de julio de 2009, que robustece la Ley 679 de 2001, definiendo en su Capítulo VI, y complementa los artículos 218 y 219 del Código Penal, impone sanciones para los "Tipos penales de turismo sexual y almacenamiento e intercambio de pornografía infantil" con penas de prisión de diez (10) a veinte (20) años y multas de ciento cincuenta (150) a mil quinientos (1.500) salarios mínimos legales mensuales vigentes (SMLMV)[9]

La Ley 1273 de 2009 complementa el Código Penal y crea un nuevo bien jurídico intermedio[10] que tutela el concepto de protección de la información y de los datos, preservando integralmente todos los sistemas basados en las tecnologías de la información y las comunicaciones. Esta ley está dividida por dos capítulos: El primero se refiere a los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. El segundo capítulo trata de los atentados informáticos y otras infracciones

---

[8] COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley 599 de 2000. Código Penal Colombiano. [en línea]. 2000. [consultado el 1º. de abril de 2020]. Disponible en: https://co.biblioteca.legal/codigo-penal/violacion-intimidad-interceptacion-comunicaciones

[9] COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley 1273 de 2009. [en línea]. 2009. [consultado el 1º. de abril de 2020]. Disponible en: https://www.oas.org/dil/esp/LEY_1336_DE_2009_Colombia.pdf

[10] Bienes Jurídicos intermedios: Son aquéllos cuya tutela va dirigida a evitar la lesión mediata o inmediata de otros bienes jurídicos [en línea] 1999. [consultado septiembre 12 de 2020]. Disponible en: https://sites.google.com/site/josycordova7/15-bien-juridico-datos-e-intimidad-personal/14-5-bien-juridico-individual-y-colectivo

Para las entidades públicas y privadas, el ordenamiento jurídico de la Ley 1273 de 2009, ha sido una importante contribución al momento de enfrentar “delitos informáticos”, esta norma define políticas y procedimientos a llevar a cabo como medida y así garantizar la seguridad de la información, de igual forma, define las acciones penales a imponer a las personas que incluyan en los delitos tipificados por la Ley. Colombia a través de esta norma se ha posicionado a la par de los países miembros de la Comunidad Económica Europea (CEE), éstos por el Convenio 'Cibercriminalidad', suscrito en Budapest, Hungría, en 2001 y vigente desde julio de 2004, ampliaron al nivel internacional los acuerdos jurídicos relacionados con la protección de la información y los recursos informáticos de los países asociados.

1.2 FORMULACIÓN

¿El ordenamiento jurídico existente en Colombia es suficiente para sancionar y penalizar las conductas ilícitas considerados como Delitos Informáticos”

2. JUSTIFICACIÓN

Motiva la realización de esta monografía la necesidad de determinar cómo los órganos impartidores de justicia han abordado delitos no tipificados en el artículo 269 del Código Penal Colombiano, delitos que cada día van en aumento y diversidad por la masificación de los medios, sistemas de información y comunicaciones, que unido a la falta de conocimiento y debido cuidado de los usuarios, los hacen presa fácil de las organizaciones de ciberdelincuentes.

Los avances científicos que han motivado el desarrollo de la humanidad han llegado posteriormente a convertirse en instrumentos tecnológicos, la utilización de estas tecnologías y sus transferencias han modificado la forma de relacionarse y su conexión con el entorno, creando ventajas competitivas, ampliando las relaciones políticas y económicas, de personas y organizaciones. A la par con el avance tecnológico surge una gran variedad de conductas ilícitas, que ponen en riesgos la estabilidad de la sociedad y que son sujeto de investigación, al igual generan nuevos tipos delictivos y amplían la modalidad de comisión de delitos tradicionales a través de medios informáticos, aumentando significativamente los bienes jurídicos que debe proteger el Legislador.

Los computadores y dispositivos móviles se han convertido en un medio valioso de comunicación, de negocios y socialización, pero a su vez son unas armas efectivas para los delincuentes, es indispensable por esta razón identificar los posibles delitos que pueden ser cometidos a través de estos medios y el cuál puede ser el tratamiento dado para su penalización. Es allí donde la seguridad informática además de ocuparse de la protección de los activos de información debe apoyar y proteger jurídicamente a las personas y las organizaciones a través de un andamiaje jurídico que ampare todos y cada uno de los aspectos de la vida de los seres humanos garantizando su seguridad o ausencia de riesgos, a medida que se presentan avances tecnológicos.

A nivel jurídico es importante profundizar el cómo se deben abordar los delitos informáticos no tipificados en el artículo 269 del CPC, a fin de determinar el tratamiento aplicable a este tipo de delitos ya que el derecho debe adaptarse a las nuevas circunstancias, esto sugiere que el Estado debe adoptar medidas jurídicas que permitan penalizar y combatir estos delitos. De igual forma, es muy importante que los profesionales no abogados, puedan identificar cuándo una conducta inapropiada puede ser tipificada como un delito informático, con el fin de estar alertas a cualquier manifestación de una actuación dañina.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Determinar si la reglamentación existente actualmente en Colombia, establecida por la Ley 1273 del 2009, que modificó el artículo 269 del Código Penal Colombiano, contiene los *elementos normativos* suficientes que permitan sancionar eficazmente las conductas asociadas a delitos informáticos.

3.2 OBJETIVOS ESPECÍFICOS

1. Revisar la normatividad vigente en Colombia sobre delitos informáticos, que permiten la identificación, definición, tipificación y penalización de estas conductas punibles.

2. Identificar las conductas delictivas cometidas mediante el uso de sistemas y/o medios electrónicos, no tipificados en la legislación colombiana como delitos informáticos, definiendo su comportamiento y la manera como están siendo abordados por las autoridades.

3. Identificar cuáles son los delitos informáticos más generalizados actualmente en Colombia, cómo es su comportamiento y las medidas que se deben tomar para su control.

4. Proponer un procedimiento para la identificación de un delito informático.

4. MARCO REFERENCIAL

4.1 MARCO TEÓRICO

La tecnología y su desarrollo evolucionan a través de la historia y hacen parte de todo tipo de actividades de la vida cotidiana, es así como, al mencionar el florecimiento de la tecnología, inmediatamente se hace referencia a la tecnología informática, la información y la comunicación. Pero este vertiginoso progreso viene acompañado de innumerables riesgos, los cuales fueron descubiertos tardíamente. Es así como, la vida social y empresarial ha sido influenciada por este avance de la tecnología informática y ha permitido el surgimiento de conductas punibles de condición dolosa llamadas de manera genérica *delitos informáticos,* que han posibilitado el surgimiento de una gran variedad de amenazas y riesgos que son de permanente estudio e investigación.

En Colombia, la Legislación Penal está regida actualmente por la Ley 599 de 2000 *Código Penal Colombiano*; Allí se describen conductas consideradas punibles, es decir, susceptibles de pena y por consiguiente merecedoras de una sanción, bien sea de arresto, multa, prisión, y otras accesorias.

Lo primero a tener en cuenta, es que la legislación tiene dentro de sus principios básicos el *Principio de Legalidad,* que establece que nadie podrá ser juzgado sino conforme a las leyes preexistentes al acto que se le imputa. Esta norma expresa que si la conducta no se encuentra descrita "exactamente dentro de un tipo penal especifico", no podrá ser juzgada por el ordenamiento penal[11]. Siendo de gran importancia la aclaración de que no siempre que una conducta parezca delincuencial, es un delito; solamente es considerada delito, aquella que ha sido tipificada como tal, por el legislador, que es la persona u órgano del cual provienen las leyes.

Igualmente se establece que, para que una conducta sea PUNIBLE debe ser tenida en cuenta por la legislación penal, además cumplir con tres elementos fundamentales del Tipo Penal: Tipicidad, Antijuridicidad y Culpabilidad.

[11] GUZMAN A. Clara L. Contextualización del cibercrimen en Colombia, 11 (28): 41-66 Vol. 4 Núm. 7, [en línea] 2009. [consultado 15 de abril de 2020], Disponible en: https://studylib.es/doc/8020365/descargar-el-archivo-pdf

Para entender con mayor precisión como se define un tipo penal, se debe tener comprensión de los siguientes conceptos:

- La Tipicidad: Es la característica de aquello que es típico (representativo o particular de algún tipo). El concepto suele utilizarse en el ámbito del derecho para nombrar a aquello que constituye un delito ya que se adecúa a una figura que describe la ley. La tipicidad supone la adecuación de una conducta a los presupuestos que detalla la legislación sobre un delito[12].

- La Antijuridicidad; se distingue por ser el acto voluntario típico que transgrede el postulado de la norma penal, lesionando o poniendo en peligro bienes e intereses tutelados por el legislador. También se puede definir como un juicio impersonal objetivo sobre la contradicción existente entre el hecho y el ordenamiento jurídico.[13]

  Dentro de la relación de Antijuridicidad y Delito, se debe tener en cuenta que no toda conducta típica es antijurídica, si bien es cierto que, en la mayoría de los casos las conductas típicas suelen ser también antijurídicas, también se pueden encontrar conductas que, aunque estén tipificadas por el Código Penal no son antijurídicas, no son delitos; es decir, son consideradas como lícitas conforme a derecho.

- La Culpabilidad: esta es una categoría de la teoría del delito la cual permite increpar la conducta de la persona que cometió un delito y por lo tanto atribuirle esa conducta y hacerle responsable de ese hecho[14].

Según Gomez-Perals en 1994, aparece un conjunto de comportamientos dignos de reproche penal que tienen por instrumento o por objeto a los sistemas o elementos de técnica informática, o que están en relación significativa con ésta, pudiendo presentar múltiples formas de lesión de variados bienes jurídicos.[15]

---

[12] PEREZ PORTO, Julián; MERINO, María, Definición de Tipicidad. [en línea]. 2016. [Consultado 15 de abril de 2020]. Disponible en: https://definicion. de/tipicidad/

[13] PINO, Francisca. Antijuricidad en el Derecho Penal, Apuntes de Derecho Penal, [en línea]. 2019. [Consultado 15 de abril de 2020]. Disponible en: https://definicion. de/tipicidad/https://www. docsity. com/es/antijuricidad-en-el-derecho-penal/4522972

[14] CULPABILIDAD [Anónimo]. [en línea]. 2003. [consultado 15 de mayo de 2020]. Disponible en: https://www.ecured. cu/Culpabilidad

[15] GÓMEZ PERALS, Miguel, Los Delitos Informáticos en el Derecho Español. [en línea]. 2003. [consultado 15 de mayo de 2020]. Disponible en: https//Dialnet-LosDelitosInformaticosEn ElDerechoEspanol-251084%20(1).pdf

Para efectos de la presente monografía se define como delitos Informáticos a un cúmulo de acciones u omisiones ejecutadas dentro del ciberespacio las cuales promueven un delito individual, social, económico, y/o político, el cual se encuentra enmarcado en el ordenamiento jurídico territorial en el que se encuentre alguna de las partes implicadas (victima(s) y/o victimario(s)[16]. Los Ciberdelitos son aquellas actividades delictivas o abusivas relacionadas con los ordenadores y las redes de comunicaciones, bien sea por utilizar el ordenador como herramienta del delito, o por que el objetivo del delito sea el sistema informático o la información allí contenida.

Los delitos informáticos están clasificados en tres grupos así: A. delitos informáticos con sentido económico, B. delitos informáticos sociales, y C. políticos o ideológicos[17].

- Los delitos informáticos económicos: son aquellas actuaciones que afectan directamente a las personas y organizaciones con o sin ánimo de lucro, y su comisión genera costos económicos o depreciaciones en el patrimonio, las cuales son ocasionadas por acciones informáticas intencionadas de terceros. Estas acciones delictivas se catalogan tres modalidades, el hurto de información, la afectación del sistema, y la falsificación para transacciones. El método Phishing es el principal causante del robo de la información y consiste en una técnica para engañar al usuario para robarle información confidencial con fines de estafa; generalmente es presentado de dos clases como lo son Smishing y Vishing, y pueden ser mediante la transmisión del mensaje y posteriormente la llamada del delincuente, con tácticas como: lo son los premios por parte de operadores de telefonía celular y almacenes de cadena, la falsas ofertas en bolsas de empleo virtuales o la falsa llamada del sobrino retenido[18].

  Otra forma de provocar estos delitos informáticos económicos, es mediante la afectación o infestación del sistema, producto por la inclusión maliciosa de un virus a los diferentes sistemas, con el fin de lograr un desfalco, los más

[16] VALDERRAMA ESTUPIÑAN, Harrisson Jahir. El Papel de las Políticas y la Normatividad en la Prevención Y Regulación del Ciberdelito [en línea].2018 [consultado 1º. de abril de 2020]. Disponible en: (https://www. gestiopolis. com/ciberdelito-politicas-publicas-y-normatividad-para-su-prevencion-en-bogota-colombia/)

[17] OJEDA-PEREZ, Jorge Eliécer; RINCON-RODRIGUEZ, Fernando; ARIAS-FLOREZ, Miguel Eugenio and DAZA-MARTINEZ, Libardo Alberto. Delitos informáticos y entorno jurídico vigente en Colombia. Cuad. Contab. vol.11, n.28, [en línea].2010. [consultado 15 de mayo de 2020]. Disponible en: https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

[18] Idem, p.3

comunes en Colombia son el Ransomware, Malware, y por medio de las APT (Amenazas Persistentes Avanzadas).

La última modalidad de este tipo de delito se presenta mediante las adulteraciones para transacciones, las cuales consisten en la falsificación de cuentas de páginas, e-mail, usuarios, etc… para que allí realicen transacciones monetarias, su principal forma de expresión en Colombia es por medio de los BEC (Business Email Compromise) que se definen "como una estafa sofisticada, destinada a las empresas que trabajan con proveedores extranjeros y/o con empresas donde se llevan a cabo los pagos a través de transferencias electrónicas internacionales"[19]. Y que procede por medio del fraude CEO, "en el que los ciberdelincuentes falsifican la dirección de correo ejecutivo de una organización, con el fin de iniciar una transferencia de fondos a sus propias cuentas"[20].

Otra manera de ejecutar alteraciones para transacciones es mediante el fraude electrónico en cajeros automáticos ATM, esta modalidad es conocida como Skimming y se ejecuta porque los ciberdelincuentes logran crear una copia de la banda magnética o chip correspondiente a una tarjeta de crédito o débito, la cual es utilizada para consumar un hecho delictivo, realizando compras o directamente retirando dinero de cuentas bancarias"[21].

- Delitos Informáticos Sociales: son una serie de acciones que causan detrimentos a la persona en "su honor, intimidad, libertad sexual o similares bienes jurídicos" [22], allí se encuentran definidos todos aquellos delitos propios del Ciberbullying, de la misma manera está la suplantación de identidad, grooming, sextorsión, instigación a delinquir, apología al delito, entre otros comportamientos inaceptables"[23]. Ocasionando daños a la persona en su buen nombre, su intimidad, la dignidad, la libertad frente a la locución y el sostenimiento de actos sexuales, la identidad sexual entre otros nuevos bienes jurídicos y se propaga fácilmente en la población vulnerable como los menores de edad, es decir a la nueva generación (los Millennials), por ser ellos quienes más hacen uso del ciberespacio para su estudio, las relaciones su comunicación, su trabajo, etc…

[19] Idem, p.4
[20] Idem, p.4
[21] Idem, p.6
[22] Idem, p. 7
[23] Idem, p.9

4.2 MARCO LEGAL

La Ley 1273 de 2009, crea un nuevo *bien jurídico intermedio* que tutela el concepto de la *protección de la información y de los datos*, tipificando en Colombia los delitos informáticos así: acceso abusivo a un sistema informático (modificado del Código Penal); obstaculización ilegítima del sistema informático o red de telecomunicación; interceptación de datos informáticos; daño informático; uso de software malicioso; hurto por medios informáticos y semejantes; violación de datos personales; suplantación de sitios *web* para capturar datos personales y transferencia no consentida de activos.[24]

Este ordenamiento jurídico, se convirtió en una importante contribución para enfrentar “los delitos informáticos”, ya que contiene definidas las políticas de seguridad de la información, algunos procedimientos y detalladas las acciones penales que se pueden adelantar en contra de las personas que incurran en este tipo de conductas.

Con los avances jurídicos hasta ahora logrados respecto de "la protección de la información y de los datos y la preservación integral de los sistemas que utilicen las tecnologías de información y comunicaciones", las diferentes entidades pueden acoger gran parte de sus sistemas integrados de información: datos, procesos, políticas, personal, entradas, salidas, estrategias, cultura corporativa, recursos de las TIC y el entorno externo[25], de manera que, además de contribuir a asegurar las características de calidad de la información, se incorpora la administración y el control, en el concepto de protección integral.

La disposición de la Ley 1273 de 2009, en el capítulo I se enfoca especialmente a afirmar la labor de los grupos de Auditoría de Sistemas, al sentar el propósito de aseguramiento de las condiciones de calidad y seguridad de la información en las entidades, cuando se refiere a los "atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos". Ratifica la relevancia de la información como activo de valor para las entidades (ISO/IEC 17799/2005), es ineludible proteger adecuadamente para avalar la continuidad del negocio, la maximización del retorno de la inversión y el aprovechamiento de las oportunidades del entorno, así como para disminuir y contrarrestar los riesgos y delitos que la amenazan.

---

[24] CONGRESO DE LA REPÚBLICA, CODIGO PENAL COLOMBIANO, Ley 599 de 2000. [en línea]. 2000. [consultado 13 de abril de 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html

[25] OJEDA P., Jorge, op cit, p. 7

A continuación, se presenta un sumario con el marco jurídico vigente en Colombia, sobre los cuales se basa el legislador, para penalizar a las personas que cometen acciones delictivas frente al manejo de información por medios electrónicos.

Tabla 1. Compendio del Marco legal en Colombia aplicable a Delitos Informáticos 2020

Normatividad	Objeto de la Norma	Aplicabilidad a los delitos Informáticos
Decreto 1360 de 1989	Por el cual se reglamenta la Inscripción del Soporte Lógico (software) en el Registro Nacional del Derecho de Autor	Es utilizado en delitos informáticos como la piratería
Constitución Política de 1991 (artículo 15)	Respetar la intimidad personal y familiar de todo ciudadano es deber del Estado, y toda persona tiene derecho a conocer toda información que se ha recogido sobre ella en cualquier base de datos, sea pública o privada.	Cualquier tipo de Ciberdelito que viole este delito será penalizado, como por ejemplo el robo de identidad y el fraude
Ley 44 de 1993	Derechos de autor	Protege los derechos de autor contra la piratería o cualquier otra modalidad de delitos relacionados con la autoría
Ley 679 de 2001	Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución.	Se aplica a delitos como pornografía infantil o trata de personas en la web.
Ley 1336 de 2009	Por medio de la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la	Se aplica a delitos como pornografía infantil o trata de personas en la web y autorregulación de los café internet

Normatividad	Objeto de la Norma	Aplicabilidad a los delitos Informáticos
	pornografía y el turismo sexual con niños, niñas y adolescentes.	
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones	Crea un nuevo bien jurídico tutelado a partir del concepto de la protección de la información y de los datos, con el cual se preserva integralmente a los sistemas que utilicen las tecnologías de la información y las comunicaciones. Se tipificaron los delitos informáticos en Colombia en los siguientes términos: acceso abusivo a un sistema informático (modificado del Código Penal); obstaculización ilegítima del sistema informático o red de telecomunicación; interceptación de datos informáticos; daño informático; uso de software malicioso; hurto por medios informáticos y semejantes; violación de datos personales; suplantación de sitios *web* para capturar datos personales y transferencia no consentida de activos
Ley 1341 de 2009	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la	Se crean unas instituciones para la regulación de los ciberdelitos en Colombia

Normatividad	Objeto de la Norma	Aplicabilidad a los delitos Informáticos
	Información y las Comunicaciones TIC, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones	
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales	Desarrolla el derecho constitucional que tienen todas las personas a conocer, en lo que se refiere el artículo 15 de la Constitución Política sobre protección de la información personal
Decreto 2693 de 2012	Por el cual se establecen los lineamentos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009, 1450 de 2011, y se dictan otras disposiciones	Define los lineamientos, plazos y términos para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el fin de contribuir a la investigación con la creación de mejores prácticas tomando como referencia los lineamientos del Estado colombiano
Decreto reglamentario 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Considerando: . . . Que la Ley 1581 de 2012 constituye el marco general de la protección de los datos personales en Colombia	Amplia y la aplicabilidad de la ley en Colombia sobre la protección de los datos personales
Documento CONPES 3701 de 2011	Propone lineamientos de política orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas	Demuestra como el Estado colombiano busca mitigar los efectos de la ciberdelincuencia a través del

Normatividad	Objeto de la Norma	Aplicabilidad a los delitos Informáticos
	que afectan significativamente al país.	establecimiento de políticas públicas.
Documento CONPES 3854 de 2016	Pretende implementar una política pública de seguridad digital.	Establece lineamientos de política para mejorar la seguridad en el internet y la ciberdelincuencia.
Norma Técnica NTC-ISO/IEC colombiana 27001	Es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.	Define los requisitos para el establecimiento, implementación, mantenimiento y mejora continua de un sistema de gestión de la seguridad de la información.

FUENTE: La Autora, basada en recopilación hecha por VARGAS ARCINIEGAS, Cristhian Francisco e información de la legislación colombiana

4.3. REVISIÓN DE LA LEGISLACIÓN EXISTENTE EN COLOMBIA SOBRE DELITOS INFORMÁTICOS TIPIFICADOS POR LA LEY

El artículo 1 de la Ley 1273 de 2009, fue incorporado en el Código Penal al Artículo 269A y complementa el tema relacionado con el "acceso abusivo a un sistema informático", este se presenta cuando aprovechando una vulnerabilidad en el acceso a los sistemas, o algunas deficiencias en la seguridad informática de las organizaciones, un pirata informático, irrumpe en ellos, bien sea para extraer alguna información o beneficio económico, o para demostrar la capacidad de hacer daño. Por lo regular estas intromisiones son realizadas por los usuarios del sistema, tal como se evidencia en los informes anuales de la PricewaterhouseCoopers, The global state information security y en estudios realizados por CISCO en el 2008, más del 40% de estos ataques son realizados por los mismos empleados de la empresa.

El artículo 269B plantea la contravención "obstaculización ilegítima del sistema informático o red de telecomunicación", esto sucede cuando un hacker informático, de forma ilegal, bloquea o impide el acceso por un periodo determinado a un correo electrónico o blog y maneja las claves electrónicas sin el consentimiento de los propietarios.

El artículo 269C establece como delito la "interceptación ilícita de datos informáticos", también considerada en el Artículo 3 del Título 1 de la Convención de Budapest de 2001. Esto acontece cuando una persona haciendo uso de recursos tecnológicos, obstruye datos sin autorización legal, en su sitio de origen, en el destino o en el interior de un sistema informático, o de emisiones electromagnéticas de un sistema electromagnético que los transmiten. [26]

Los "daños informáticos" están relacionados como delitos está en el Artículo 269D y se cometen cuando usando recursos de las TIC, una persona que no autorizada, altera, borra, modifica, suprime daña o destruye datos de programas o de documentos electrónicos.

El delito vinculado con el "uso de software malicioso", se encuentra estipulado en el artículo 269E, técnicamente designado como malware, ya divulgado en internet. Se ostenta cuando se producen, adquieren, venden, distribuyen, envían, introducen o extraen del país software o programas de computador que producen daños en los recursos de las TIC [27].

El delito sobre "violación de datos personales" (hacking) lo expresa el artículo 269F y está encauzado a proteger los derechos fundamentales de la persona (como dignidad humana y libertad ideológica). Se presenta, cuando un individuo sin autorización, sustrae, vende, envía, compra, divulga o emplea datos personales almacenados en ficheros, archivos, bases de datos o medios similares con el fin de lograr utilidad personal o para otros. [28].

El artículo 269G trata de la "suplantación de sitios web para capturar datos personales". Acontece cuando el suplantador (phisher) o delincuente informático crea una página y un dominio similar al de la entidad a la cual desea abordar, lo ubica en un hosting (espacio en un servidor) desde donde envía correos spam o engañosos (por ejemplo, empleos). Al no distinguir la página original de la falsa, las personas inocentemente suministran información personal y claves bancarias que el suplantador almacena en una base de datos y luego ordena la transferencia del dinero de la víctima a cuentas de terceros quienes prestan sus cuentas o servicios (testaferros), que luego reclama o distribuye. [29].

Revisada la normatividad colombiana sobre delitos informáticos, se obtuvo la información que se detalla en la siguiente tabla:

---

[26] Idem
[27] Idem
[28] Idem
[29] idem

Tabla 2. Esquema de la Ley 1237 de 2009 (Protección de Información y de los datos)

Artículo en el CPC	Delito	Cuándo se presenta	Pena
269 A	Acceso abusivo a sistemas informáticos	Aprovechan la vulnerabilidad en el acceso a los sistemas de información o debilidades en los procedimientos de seguridad	Prisión de 48 a 96 meses y multa de 100 a 1. 000 smlmv
269B	Obstaculización ilegítima de sistema informático o red de Comunicaciones	Bloquean de forma ilegal un sistema o impiden su ingreso, igualmente, el acceso a cuentas de correo electrónico de otras personas; sin el debido consentimiento	Prisión de 48 a 96 meses y multa de 100 a 1. 000 smlmv
269C	Interceptación ilícita de datos informáticos	Obstruyen datos sin autorización legal, en su sitio de origen, en un destino o en el interior de un sistema informático	Prisión de 36 a 72 meses
269D	Daños informáticos	Cuando una persona que sin estar autorizada, modifica, daña, altera, borra, 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 1. 000 smlmv
269E	Uso de software malicioso	Cuando se producen, adquieren distribuyen, envían, introducen o extraen del país software o programas de computados que produce daños en los recursos de TIC	Prisión de 48 a 96 meses y multa de 100 a 1. 000 smlmv
269F	Violación de datos personales	Sin estar facultado sustrae, vende, envía, compra, divulga, o emplea datos personales	Prisión de 48 a 96 meses y multa de 100 a 1. 000 smlmv

Artículo en el CPC	Delito	Cuándo se presenta	Pena
		almacenados en medios magnéticos	
269G	Suplantación de sitios web para capturar datos personales	delincuente informático crea una página y un dominio similar al de la entidad a la cual desea abordar, lo ubica en un hosting (espacio en un servidor) desde donde envía correos spam o engañosos (por ejemplo, empleos). Al no distinguir la página original de la falsa, las personas inocentemente suministran información personal y claves bancarias	Prisión de 48 a 96 meses y multa de 100 a 1. 000 smlmv
218	Pornografía con menores de 18 años	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.	Prisión de 10 a 20 años y multa de 150 a 1500 salarios mínimos

FUENTE: La Autora, de información tomada del Art. Delitos informáticos y entorno jurídico vigente en Colombia.

4.4 DELITOS COMETIDOS MEDIANTE EL USO DE SISTEMAS O MEDIOS ELECTRÓNICOS NO TIPIFICADOS COMO DELITOS INFORMÁTICOS.

Baón Ramírez define como criminalidad informática a todo aquel conjunto de actividades que, reuniendo los requisitos que delimitan el concepto de delito, se ejecuten esgrimiendo un elemento informático (mero instrumento del crimen) o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software (en éste caso lo informático es finalidad).[30] Se considera que no necesariamente aparecen nuevos "delitos", sino más bien ante una nueva forma de llevar a cabo los delitos tradicionales, razón por la cual no cabe individualizarlos de una manera específica, dejando de presente que el legislador deberá introducir las modificaciones legales pertinentes a fin de permitir la adecuación de los tipos tradicionales a las nuevas circunstancias.[31]

En la tabla 3 se presentan los delitos tradicionales tipificados por el CPC y que eventualmente son cometidos por el uso de medio de informáticos

Tabla 3. Delitos tradicionales cometidos mediante medios informáticos

Norma	Artículo	Delito	Cuándo se presenta	Pena
CPC	193	Ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas	Sin permiso de autoridad ofrezca, venta o compra de instrumento apto para interceptar la comunicación privada	Multa
CPC	194	Divulgación y empleo de documentos reservados	El que en provecho propio o ajeno y con perjuicio de otro divulgue o emplee el contenido de un documento reservado	Multa

[30] BAÓN RAMÍREZ, Rogelio. Visión general de la informática en el nuevo Código Penal, en Ámbito jurídico de las tecnologías de la información, Cuadernos de Derecho Judicial, Escuela Judicial/Consejo General del Poder Judicial, Madrid, [en línea]. 1996. [consultado 17 de mayo 2020]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=552416

[31] ALCURIO DEL PINO, Santiago. Delitos informaticos .[en línea]. 2014. [consultado 17 de mayo de 2020]. Disponible en: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Norma	Artículo	Delito	Cuándo se presenta	Pena
CPC	196	Violación ilícita de comunicaciones o correspondencia de carácter oficial	Quien ilícitamente sustraiga, oculte extravíe, destruya, intercepte o controle o impida comunicación de carácter oficial destinada a la rama judicial o a organismos de control o seguridad del Estado	Prisión de 3 a 6 años
CPC	197 modificado Ley 1453 de 2011	Utilización ilícita de redes de comunicaciones	El que con fines ilícitos posea o haga uso de equipos terminales de redes de comunicación o cualquier otro medio electrónico diseñado o adaptado para emitir y recibir señales	Prisión de 4 a 8 años
CPC	270	Violación a los derechos morales de autor	Publique, total o parcialmente sin autorización previa y expresa una obra inédita. Inscriba en el registro de autor con el nombre de una persona distinta o lleve a cabo cualquier modificación a una obra literaria. Por cualquier medio compendie mutile o transforme una obra de carácter literario.	Prisión de (2) a (5) años y multa de (20) a (200) smmlv.
CPC	271	Violación de derechos patrimoniales de autor y derechos conexos	Por cualquier medio o procedimiento reproduzca una obra de carácter literario, científico, artístico o cinematográfico, etc; cualquier título de dichas reproducciones.	Prisión de (4) a (8) años y multa de (22.66) a (1.000) smmlv
CPC	272	Violación a los mecanismos de protección de	El que eluda, fabrique, suprima, distribuya, importe, ensamble,	Prisión de (4) a (8) años

Norma	Artículo	Delito	Cuándo se presenta	Pena
		derechos de autor y derechos conexos y otras defraudaciones.	recepcione y presente declaraciones o informaciones destinadas directa o indirectamente al pago, recaudación. liquidación, etc.	y multa de (26.66) a (1.000) smmlv

FUENTE. La Autora, basada en el Código Penal Colombiano, Ley 509 de 2000

En los últimos años, la identificación y tratamiento de los delitos informáticos, ha recibido mucha atención, si se tiene en cuenta que aún falta claridad en la interpretación de la Ley, se observa con asiduidad, que se confunde el delito con la técnica utilizada para cometerlo. Un patrón es el caso, cuando se oye decir, que fue víctima del delito de amenaza por medios electrónicos con fines lucrativos, esto sucede cuando de manera subrepticia, alguien llama o se comunica por medio electrónico a otra persona y le solicita cancelar una suma de dinero por hacer o dejar de hacer algo, si bien es cierto que existe una amenaza, se puede decir que este no es el delito, el delito es la extorsión, de acuerdo con el artículo 244 CPC. Situaciones como ésta han dificultado no sólo la definición de delito informático, sino su interpretación para un adecuado tratamiento jurídico e institucional.

En la Tabla No.4 se presenta una serie situaciones como las referidas en el párrafo anterior donde se presentan como conductas delictivas, algunos medios informáticos o técnicas para cometerlos.

Tabla 4. Conductas delictivas cometidas por medios informáticos

		Como es judicializada	
Medio	**Delito**	**Artículo CPC**	**Pena**
Clonación de Tarjetas	Violación de datos personales	269F	48 a 96 meses de prisión multa de 100 a 1000 smlmv
Challenge o retos suicidas	Inducción o ayuda al suicidio	107	2 a 6 años de presión
Plataformas Webcam	Inducción a la prostitución	213	10 a 22 años 66 a 750 salarios mínimos
Ciber bulling	Injuria	220	1 - 3 años de prisión 10 a 1.000 smlmv

Medio	Delito	Como es judicializada Artículo CPC	Pena
	Calumnia	221	1 – 4 años de prisión, de 10 a 1.000 smlmv
Amenaza por medios electrónicos con fines lucrativos	Extorsión	244	12 a 16 años de prisión 600 a 1200 smlmv
Envío correos electrónicos desde la cuenta de terceros	Violación de datos personales	269F	48 a 96 meses de prisión multa de 100 a 1000 smlmv

Fuente: La Autora, CPC.

4.4.1 Cooperación internacional en la lucha contra la ciberdelincuencia**.** En el propósito de las naciones de luchar contra la ciberdelincuencia, para prevenir los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos redes y datos informáticos así como el abuso de dichos sistemas redes y mediante la tipificación de esos actos, y la asunción de poderes suficientes para luchar de forma efectiva contra dichos delitos, facilitando su detección, investigación y sanción tanto a nivel nacional como internacional y estableciendo disposiciones que permitan una cooperación internacional rápida y fiable; se firmó el convenio en la Ciudad de Budapest, Hungría, al cual se adhirió Colombia, 17 años después, mediante Ley No.1928 de 24 de julio de 2018, por medio de la cual se aprueba el «convenio sobre la Ciberdelincuencia», adoptado el 23 de noviembre de 2001, en Budapest, Hungría. Este convenio propone a las naciones que adopten medidas que tipifiquen y penalicen los delitos definidos en la tabla 5.

Tabla 5. Delitos definidos en el Convenio de Budapest, 2001

Tipo de Delito	Artículo	Delito	Se Comete cuando	Adoptado en Colombia por
Delitos contra la confidencialidad. la integridad y la disponibilidad de	2	Acceso ilícito	Se Infringen medidas de seguridad con la intención de obtener datos informáticos o	Adoptado por la Ley 1273 y CPC Artículo 269A

Tipo de Delito	Artículo	Delito	Se Comete cuando	Adoptado en Colombia por
los datos y sistemas informáticos			con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático	
	3	Interceptación ilícita	la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos	Adoptado por la Ley 1273 y CPC Artículo 269B
	4	Interferencia en los datos	La comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos.	Adoptado por la Ley 1273 y CPC Artículo 269C
	5	Interferencia en el sistema	Se adoptarán las medidas necesarias ante: la obstaculización grave, deliberada e ilegitima del funcionamiento de un sistema	Adoptado por la Ley 1273 y CPC Artículo 269D

Tipo de Delito	Artículo	Delito	Se Comete cuando	Adoptado en Colombia por
			informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos.	
	6	Abuso de los dispositivos	la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de un dispositivo, programa informático…	No se encuentra explícitamente concebido en el Código Penal Colombiano, como delito informático.
Delitos Informáticos	7	Falsificación informática	cuando se cometa de forma deliberada e ilegítirna, la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténtico	Se encuentra expreso en el artículo 269 incisos: A, F, G y J.
	8	Fraude informático	Lo actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante:	Se encuentra expreso en el artículo 269 incisos: F, I y J.

Tipo de Delito	Artículo	Delito	Se Comete cuando	Adoptado en Colombia por
			a. Cualquier introducción, alteración, borrado o supresión de datos informáticos y b. Cualquier interferencia o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona.	
Delitos relacionados con el contenido	9	Delitos relacionados con pornografía infantil	La producción de pornografía infantil con intención de divulgarla La oferta opuesta a disposición de pornografía infantil a través de un sistema informático La difusión y o la transmisión de pornografía infantil….	Artículo 218 CPC
Delitos relacionados con la propiedad intelectual y Derechos afines	10	Delitos relacionados con la propiedad intelectual y Derechos afines	Derechos de autor, Derechos de propiedad intelectual; derecho de los artistas	Art. 270 CPC

Fuente: La Autora, CPC.

Al respecto cabe señalar que Colombia ya había avanzado desde el año 2009 con la expedición por el Senado de la República de la Ley 1273, por medio de la cual se incorporó al Código Penal un nuevo bien jurídico tutelado denominado “de la protección de la información y de los datos”, por lo que se puede decir que el país ya traía tarea adelantada por lo menos en relación con el capítulo del convenio que protege el CID, antes de la firma en el 2018.

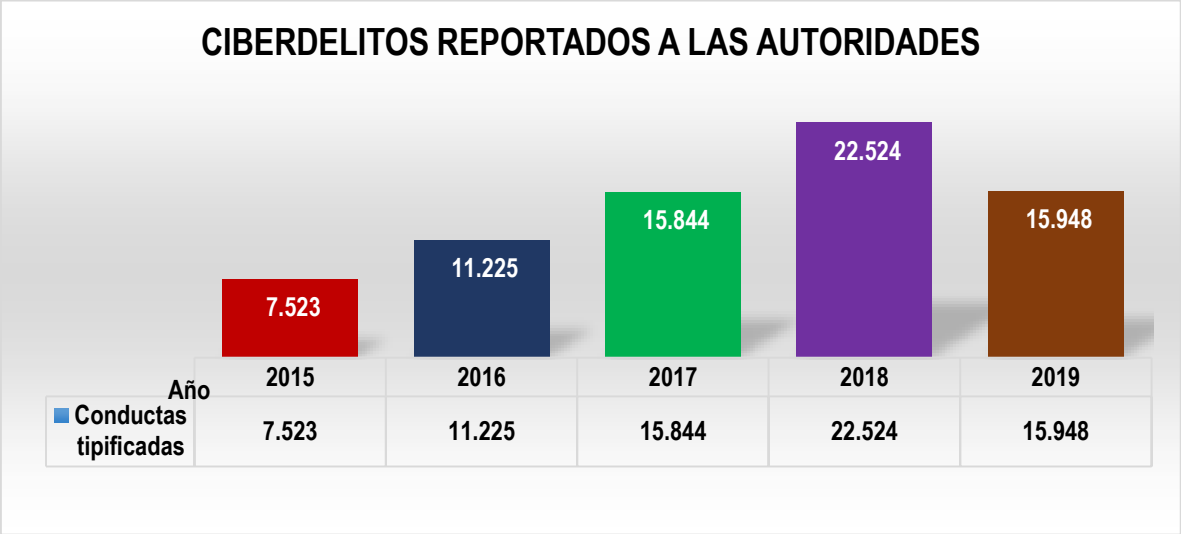
4.5 DELITOS INFORMATICOS MÁS GENERALIZADOS EN COLOMBIA

La dinámica de los delitos informáticos presenta un perfeccionamiento exponencial, esto ha apoyado que delincuentes que inicialmente procedían de forma aislada, sin coordinación, con un alcance local, actualmente se hayan constituido en complejas organizaciones trasnacionales de Cibercrimen. No obstante, de haber transcurrido más de treinta años desde que comenzó a hablarse de la criminalidad informática, y más de veinte desde que se acuñó el término Cibercrimen, parece que el fenómeno de la criminalidad relacionada con el uso de las Tecnologías de la Información y la Comunicación sigue siendo totalmente novedoso y por ello, parcialmente incomprendido por la sociedad en general y, en particular, por las instituciones encargadas de la prevención de esta amenaza.

De acuerdo con el estudio "Tendencias del Cibercrimen 2019-2020", presentado por el Tanque de Análisis y Creatividad de las TIC - TicTac de la CCIT y su programa SAFE en asocio con la Policía Nacional - Centro Cibernético Policial[32], durante el periodo 2015 – 2019 se presentó el siguiente comportamiento de los ciberdelitos reportados a las autoridades que se representan en la Figura 1.

[32] TANQUE DE ANÁLISIS Y CREATIVIDAD DE LAS TIC - TICTAC DE LA CCIT, El estudio Tendencias del Cibercrimen 2019-2020. [en línea]. 2020. [Consultado 3 de noviembre de 2020]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Figura 1. Colombia. Ciberdelitos reportados a las autoridades 2015-2019



Fuente: La Autora. Información de la Revista Tendencias del Cibercrimen 2019-2020

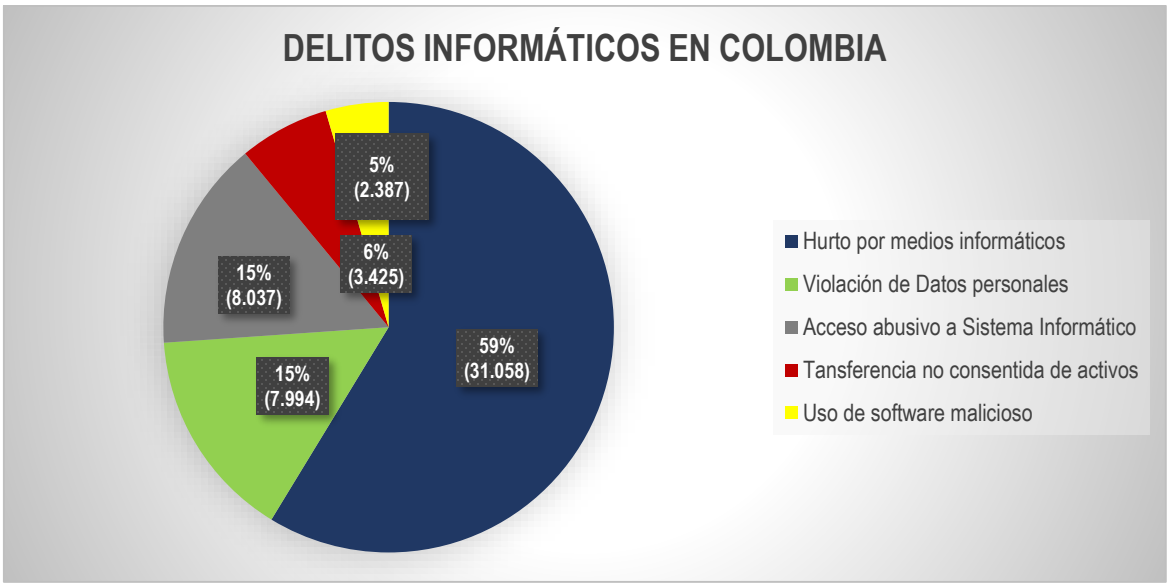
Según la información proporcionada por la fuente mencionada anteriormente, la dinámica del Cibercrimen presenta un crecimiento gradual en el registro de reportes de la ciudadanía a los sistemas de seguridad, de acuerdo con este mismo reporte en el año 2019 se presentaron 28.827 denuncias, de las cuales 15.948 casos fueron catalogados como infracciones a la Ley 1273 de 2009, que corresponde al 57%.

Del total de las denuncias, el 54.5% fueron presentadas de manera presencial y un 45.5% se realizaron de manera virtual a través de la aplicación *ADenunciar,* que fue puesta al servicio desde julio de 2017.

4.5.1 Principales delitos informáticos que suceden en Colombia. La información presentada se puede establecer que el principal interés que se presenta en Colombia de cometer delitos informáticos es netamente económico, que se cristaliza con la posterior monetización del resultado del ciberataque.

Con base en la información reportada por los colombianos en el aplicativo *ADenunciar,* desde mediados de 2017 hasta el 2019 se han reportado 52.901 casos los cuales están catalogados como se representa en el Figura 2.

Figura 2. Principales delitos informáticos presentados en Colombia 2017-2019



Fuente: La Autora. Información de la Revista Tendencias del Cibercrimen 2019-2020

El delito con más frecuencia cometido en Colombia es el *Hurto por medios informáticos*, con un 31.058 (59%) de los casos; los delincuentes conocen del manejo de las operaciones bancarias y saben que el dinero está en los bancos por tal razón, interfieren de manera fraudulenta comprometiendo los dispositivos mediáticos entre el banco y sus clientes. Para el 2019 la denuncia de este delito disminuyó al 28%, ya que para las reclamaciones a los bancos no se requiere la denuncia previa.

En segundo lugar, se encuentra ubicado el delito de *violación de datos personales*, también llamado *Robo de Identidad,* en este periodo se presentaron 7.994 (15%) casos, para el 2019 este delito presentó un incremento considerable al llegar al 42% de los casos reportados.

El tercer delito más denunciado es el *Acceso abusivo a sistema informático*, se reportaron 7.994 (15%) casos, este delito es muy común en las fases primarias de los ciberataques los delincuentes ingresan a los sistemas de información, una vez allí pueden realizar los ataques.

En cuarto lugar, se encuentra la *Transferencia no consentida de activos*, en el periodo se presentaron 3.425 (6%) casos, esta modalidad de delito permite transferir valiosos activos de las víctimas a otras cuentas fraudulentas.

En último lugar se encuentra el *Uso de software malicioso,* con una incidencia de 2.387 (5%) casos. Este delito tuvo un gran incremento en el 2019 al presentarse el en 14% de las denuncias[33].

4.5.2 Delitos informáticos por ciudades. Con la penetración del internet a la mayor parte de los rincones de Colombia, ha facilitado el despliegue del fenómeno criminal, sin embargo, las mayores ocurrencias reportadas se encuentran ubicadas en las ciudades y centros urbanos donde se instalan las PYMES, grandes compañías, entidades financieras, cooperativas. Para el 2019, el 55% de los delitos informáticos ocurrieron en las siguientes ciudades: Bogotá 5308 casos, Cali 1.190, Medellín 1.186, Barranquilla 643 y Bucaramanga 397. La ingeniería social es la causante de cerca del 90% de los ciberataques perpetrados a las entidades que funcionan en Colombia.

4.6 PRINCIPALES MODALIDADES DE CIBERCRIMEN EN COLOMBIA

4.6.1 Los ataques BEC. Los ataques BEC, por sus siglas en inglés, Business Email Compromise, es una de las principales amenazas que se presentan en la cadena de suministros a una empresa y hacen parte de ´su actividad diaria, para lograr una mayor eficiencia se requiere de una constante y muy segura comunicación con sus proveedores y clientes. Es así como los ciberdelincuentes aprovechando las debilidades en los sistemas de información y correos electrónicos logran conseguir que, mediante la suplantación de ejecutivos, algunos empleados realicen acciones no autorizadas que conlleven a la defraudación de la empresa, todo esto mediante la utilización de ingeniería social.

En el 2019 los ataques BEC, lideran las denuncias recibidas por las autoridades de las diferentes estafas, las principales son las siguientes: Correos Fraudulentos Personalizados (Spear Phishing); Suplantación de identidad; Enmascaramiento de correos (Spoofing); Infección de sitios frecuentemente visitados por empleados (Watering Hole)[34].

Las principales modalidades de ataques BEC se encuentran las siguientes: *Estafa de CEO o suplantación del Gerente:* esto sucede mediante correo malicioso que se apodera de la cuenta de correo del gerente se envían correos a los empleados encargados de realizar los pagos y dispensar los fondos y así realizar las transferencias a las cuentas falsas. *Suplantación de clientes:* mediante correos engañosos se realizan los cobros de facturas y el recaudo se hace en las cuentas

[33] Ibidem, pág. 7

[34] Ibidem pág. 11

de los *mone*, que son personas que prestan sus cuentas para que se cometan estos tipos de delitos.

4.6.2 Ransomware. Aunque esta no es una modalidad reciente, en Colombia ha venido en aumento esta modalidad de delito por el incremento en el uso de las criptomonedas como medio para monetizar las ganancias del Cibercrimen a nivel mundial. De acuerdo con la información de 2019 de INTERPOL, en Colombia se sucedieron el 30% de los ataques de Latinoamérica, seguido por el 16% del Perú, 14% de México, 11% del Brasil y un 9% en Argentina. Es así como, de acuerdo con la información suministrada por el Centro Cibernético Policial, 717 empresas colombianas reportaron ataques exitosos de Ransomware en este mismo año, siendo las PYME las de mayor afectación ya que estas pequeñas y medianas entidades carecen de protocolos de respuesta a la violación y de políticas de seguridad y privacidad de la información.

En Colombia se han detectado principalmente 5 clases de Ataques: 1) *Ransomware de cifrado*: Se caracteriza por cifrar archivos personales y documentos, tales como videos, imágenes y hojas de cálculo. 2) Ransomware de cifrado de servidores web; Su principal intención son los servidores web y cifrar sus archivos. 3) Lock Screen Ransomware WinLocker: Impide el acceso a la pantalla del PC y solicita un pago para desbloquearla. 4) *Master Boot Record (MBR) Ransomwarealware*: Se encarga de bloquear la parte del disco duro del PC que permite iniciar el sistema operativo. 5) *Ransomware de dispositivos móviles*: Son objeto de ataques teléfonos celulares (principalmente Android) y se infectan mediante descargas no oficiales.[35]

[35] Ibidem, pág 14

4.6.3 DDOS Ataque de denegación del servicio. Son implementados con el principal objetivo de inhabilitar un servicio designado por un servidor, creando un colapso en el sistema beneficiándose de sus vulnerabilidades. Pueden tener su origen por fallas en la configuración o por el accionar malintencionado de empleados inconformes. En el 2019, Según cifras del Centro Cibernético Policial, 170 empresas reportaron ataques DDoS que consiguieron interrumpir sus servicios de cara a sus clientes; según esta misma fuente los ciberdelincuentes estaban motivados por los siguientes factores: Reconocimiento y escaneo de los servicios de la compañía a afectar; Utilización de redes Botnet para lanzar ataques dirigidos a los servicios online; Interrupción de los servicios para los usuarios y terceros (clientes); Exigencia a través de correo electrónico o chat de ciberextorsión; Solicitud y demanda de pagos en criptomonedas, principalmente Bitcoins.[36]

4.6.4 Malware. Es un software malicioso regularmente maligno que trata de afectar los computadores, teléfonos celulares o cualquier otro tipo de dispositivo. En Colombia en el 2019 esta modalidad de software malicioso se incrementó con respecto al año anterior en un 612%, al pasar de 99 casos reportados en el 2018 a 705 en el 2019, siendo las PYME las más afectadas.[37]

4.6.5 SIM SWAPPING, secuestro o cambio de Sim Card. Las tarjetas SIM presentan una gran vulnerabilidad y es el hecho que desempeñan bajo cualquier plataforma, lo ejecuta mediante lo que se distingue como “ingeniería social”, esto hace que los vendedores de empresas de celulares se confundan y trasladan los números a tarjetas controladas por ellos. En Colombia se reporta el robo de 99 celulares cada hora. Con los celulares robados solicitan al operado una nueva tarjeta SIM; Lo más ininteligible del asunto es que los criminales emplean la “nueva” SIM CARD, para tener acceso a cuentas financieras que usan autenticación de dos factores a través de mensajes de texto (2FA).[38]

4.6.6 Cryptojacking minería de criptomonedas. El Cryptojacking es un plan para utilizar los dispositivos de otras personas (ordenadores, teléfonos inteligentes, tabletas o incluso servidores), sin su consentimiento ni su conocimiento, para extraer criptomonedas subrepticiamente a costa de la víctima.

4.7. MEDIDAS A TOMAR PARA CONTROLAR LA PROPAGACIÓN DE DELITOS INFORMÁTICOS.

Es importante que tanto personas como empresas tomen conciencia de proteger su información, ya que se tiene registro que el 60% de las pequeñas y medianas

[36] Ibidem pág. 18

[37] Ibidem pág.20

empresas, no pudieron sostener sus negocios después de seis meses de haber sufrido un ciberataque importante. Los Ciberataques a PYMES en Colombia comprometen seriamente los activos económicos e impactan asuntos estrictamente legales y de cumplimiento de las compañías.[39] Consecuentemente, se deben adoptar una serie de normas y medidas preventivas para evitar que los ciberataques puedan afectar de manera directa a empresas y personas; Para revenirlas se debe tener en cuenta lo siguiente:

a) El Estándar ISO/IEC 27701, presentado recientemente tiene como objeto dar orientaciones acerca del resguardo de la privacidad, que incluye la protección que las empresas deben dar a la información personal, está definido a nivel mundial como el Reglamento General de Protección de Datos. Es así como, las compañías que no tengan definida e implementada un Sistema de Gestión de Seguridad de la Información –SGSI, pueden implantar las normas ISO/IEC 27001 e ISO/IEC 27701 paralelamente.
b) Evitar realizar tareas sensibles para la organización desde el teléfono celular, como lo es el correo electrónico corporativo, porque puede perderse información valiosa para la compañía.
c) Se debe implementar una apropiada política de almacenamiento de información en la nube, definiendo el tipo de información y el tiempo de permanencia en los repositorios virtuales.
d) Se debe definir el uso del correo corporativo, para actividades estrictamente empresariales, evitando circular aplicaciones de juegos, ocio o citas.
e) Guardar una regulación directa en la política de proveedores y clientes; como también del manejo de estos con la ciberseguridad de la empresa.
f) Es muy importante establecer mecanismos perimetrales de protección como antivirus, antimalware, anti-fishing indispensables en la infraestructura del negocio.
g) Si la empresa ha sido víctima de algún ataque debe desarrollar la capacidad de ciberresiliencia aplicándola en las tres áreas críticas: seguridad de la información, la continuidad del negocio y la capacidad de recuperación de la organización.
h) Si la empresa aún no ha sido víctima de ningún ataque, debe prepararse para afrontar este tipo de situaciones, definiendo los roles y compromisos que tiene cada uno de los actores involucrados en el plan de respuesta y gestión de un incidente cibernético.

[38] Ibidem pág. 25

[39] Ibidem, pág. 31

4.8 ANÁLISIS DE CASOS DE JUZGAMIENTO A DELITOS INFORMÁTICOS EN COLOMBIA

Caso 1. De Hurto por medios Informáticos: La Sentencia 34564 del 25 de agosto de 2010, sobre la competencia para juzgar en un delito de Transferencia de Activos presentado así, el 28 de mayo de 2009, originada desde la ciudad de Barranquilla, de manera ilícita y superando barreras electrónicas, se trasfirió a varios destinos bancarios (nueve cuentas) la suma de ciento nueve millones de pesos ($109.000.000.oo) que estaban en una cuenta de Bancolombia, de la Oficina ubicada en el Centro Comercial Campanario de la ciudad de Popayán, de propiedad del mismo Centro Comercial. Como consecuencia de la investigación coordinada por la Fiscalía Séptima Seccional Adscrita ante la URI de Barranquilla, se logró la individualización de WILFRIDO FONTALVO HERNANDEZ, ISAIT EDUARDO HERNANDEZ MEDRANO, FEDERICO SANTODOMINGO HERRERA, DEIVIS GABRIEL OLAYA y EMIGDIO CORRO CASTAÑEDA a quienes se les imputó hurto calificado (por haberse cometido superando seguridades electrónicas según lo dispuesto en el artículo 240.4 del Código Penal) con circunstancia de mayor punibilidad (por cuanto fue cometido en coparticipación criminal); Los implicados aducían que el juzgado penal de Popayán no tenía la competencia para llevar el caso; a lo cual La Suprema Corte de Colombia, en su Sala de Casación Penal, deja claramente expreso que: a) como el delito se consumó en la ciudad de Popayán, es la autoridad judicial de tal distrito judicial la llamada a juzgarlo; y, b) de acuerdo con el artículo 1º de la Ley 1273 de 2009 el delito corresponde a la denominación de “hurto por medios informáticos y semejantes” fallando que la competencia para adelantar el juzgamiento correspondiente a esta actuación procesal corresponde a un Juzgado Penal Municipal con Funciones de Conocimiento de la ciudad de Popayán; por lo que se remitirán las diligencias al Centro de Servicios Judiciales de dicha ciudad para el correspondiente reparto.[40]

Caso 2. En el año 2014, en periodo de elecciones presidenciales en Colombia, fue noticia nacional la captura de Andrés Fernando Sepúlveda Ardila, conocido como el “el hacker”, señalado de pertenecer y liderar una oficina de interceptaciones ilegales en el país, es acusado de “monitorear ilegalmente el proceso de negociación de la Habana, a través de correos y extracción de documentación por medio de técnicas

[40] COLOMBIA. CORTE SUPREMA DE JUSTICIA, Sala de Casación Penal, [en línea]. 2010. [consultado diciembre 1o. De 2020]. Disponible en: https://es.slideshare.net/Alediaganet/sentencia-34564-25-08-10-competencia-transferencia-activos

de HACKIN, en la oficina ubicada en la ciudad de Bogotá.[41] "El 10 de Abril del 2015, el juzgado 22 penal de circuito de conocimiento realizó audiencia y conoció la sentencia Condenatoria contra Andrés Fernando Sepúlveda, quien es condenado por medio de la figura del preacuerdo, a diez años de prisión, por los delitos de Espionaje, Concierto para delinquir agravado, Acceso abusivo a un sistema informático, Uso de software malicioso y Violación de datos personales agravado, en calidad de coautor material. A manera que, la ejecución de estos delitos es debido al uso de software malicioso, el ingreso a cuentas de correo electrónico con el fin de obtener información de diferentes personas, usando redes sociales con fines de interceptación de datos informáticos y acceso abusivos a los sistemas de información. Además, es importante mencionar que, esta es la "Primera Condena por Espionaje" en la historia de Colombia.[42]

Caso 3. Otro caso de renombre nacional fue conocido en el 2018, cuando Jaime Alejandro Solano Moreno, conocido como el "Rey millas", quien mediante maniobras ilícitas ingresaba de manera fraudulenta a las páginas web de las aerolíneas, utilizando las "millas aéreas" de famosos como artistas, políticos, personas en general que obtenía por medio de la consumación de estos delitos las convertía en tiquetes aéreos para sí mismo; una vez capturado le fueron imputados los cargos de violación de datos personales (ART 269F) y hurto informático (ART 269I). Las pérdidas económicas en este caso superan los $541.000.000.[43]

Caso 4. Una masajista entró a laborar en un servicio de masajes relajantes. Al momento de vincularse le solicitaron realizar un estudio fotográfico y tuvo que firmar una autorización para la circulación y publicación de las fotos. El jefe de inmediato la presionaba para que brindara a los clientes la opción de "pasar a otro nivel de masajes", lo cual extralimitaba sus funciones, razón por la cual decidió renunciar y desvincularse de la empresa. Al presentar la renuncia solicitó retirar las fotos de las redes sociales y de la publicidad de la empresa, así como la devolución de las mismas, a lo cual la empresa se negó indicando tener derecho en virtud de la

[41] FISCALÍA GENERAL DE LA NACIÓN, Proceso de Investigación y judicialización. [en línea]. 2015. [consultado diciembre 1o. De 2020]. Disponible en: https://www.fiscalia.gov.co/colombia/wp-content/uploads/20170111.pdf

[42] Ibidem, pag.17

[43] REVISTA SEMANA, CIBERCRIMEN, El 'rey millas' que le dio la vuelta al mundo a cuenta de Sofía Vergara, Juanes y otros famosos. [en línea] 2018 [Consultado diciembre 3 de 2020]. Disponible en: emana.com/tecnologia/articulo/jaime-alejandro-solano-moreno-el-rey-millas-que-viajo-por-cuenta-de-sofia-vergara-juanes-y-otros-famosos/561833/

autorización. Acorde con esto, presentó una tutela argumentando que, si bien había autorizado, actualmente considera que afecta sus derechos fundamentales. La Corte Constitucional explicó que la autorización para que terceros usen la imagen personal de alguien no significa renunciar de manera indefinida a disponer de ella, por lo que ordenó tutelar los derechos y retirar las imágenes.; la corte también argumentó que fueron vulnerados loa derechos a la propia imagen, honra, buen nombre e intimidad. y como sanción se impuso: retirar de Facebook y de cualquier otro medio de publicidad las imágenes de la accionante y abstenerse de divulgarlas y publicarlas.[44]

Caso 5. La madre de una niña de cuatro años de edad presentó una acción de tutela al considerar que el padre, al abrirle una cuenta en Facebook, le vulneró varios derechos a la menor. Según la progenitora, por la corta edad de la niña no contaba con la madurez necesaria para abrir por su propia voluntad un perfil. El padre sostuvo que lo creó para mantener contacto con su hija, ya que, debido a problemas con la madre, transcurrían largas temporadas sin que la pudiera ver. La Corte Constitucional indicó que la niña no está en capacidad de dar su consentimiento previo, expreso e informado para acceder a esta red social; ya que vulnera el derecho a la intimidad, buen nombre y libre desarrollo de la personalidad de la menor; colocando como sanción: cerrar el perfil de Facebook y no crear una cuenta en una red social con datos de la hija.[45]

Caso 6. El ‘Mono Jojoy’ abatido 23 de septiembre de 2010, en la ‘Operación Sodoma’, lanzada por el Ejército colombiano contra la fortaleza del jefe guerrillero enclavada en las selvas del sur del país. La información de los computadores del ‘Mono Jojoy’ y la de los de Luis Edgar Devia, alias ‘Raúl Reyes’, muerto en marzo de 2008 tras un ataque del Ejército a un campamento de las FARC en territorio ecuatoriano, sirvieron a la inteligencia colombiana para conocer más las estructuras de las FARC y combatirlas. Sin embargo, en mayo del 2011, la Corte Suprema de

[44] REVISTA AMBITO JURÍDICO, Las insólitas condenas por el mal uso de las redes sociales [en línea] 2017 [Consultado diciembre 3 de 2020]. Disponible en: https://www.ambitojuridico.com/noticias/tic/las-insolitas-condenas-por-el-mal-uso-de-las-redes-sociales

[45] Ibidem, pág. 6

Justicia determinó que el material encontrado en los computadores de Reyes no podría ser utilizado como pruebas porque fue recolectado ilegalmente [46]

4.9 PROCEDIMIENTO PARA LA IDENTICACIÓN DE UN DELITO INFORMÁTICO

El Código penal define el procedimiento para la identificación de una conducta inapropiada como delito, para poder tipificarlo como tal la conducta debe cumplir con unos requisitos denominados elementos del tipo penal, los cuales son definidos de la siguiente manera:

4.9.1 Elementos del tipo penal

4.9.1.1 Supuesto Lógico

Son los presupuestos necesarios para acreditar la existencia de los distintos delitos en lo particular. Por ejemplo, en el delito de Acceso abusivo a un sistema informático: La existencia previa de un sistema de información. [47]

4.9.1.2 Verbo Rector

El verbo es la parte más importante de una oración. La conducta descrita en el tipo se plasma en una oración gramatical. La forma verbal que nutre antológicamente la conducta típica de tal manera que ella gira en derredor del mismo. La importancia de lo dicho radica en que la interpretación que sobre la norma hacen jueces, magistrados, fiscales y abogados. La oración o norma conducta, puede tener varios verbos, pero solo uno será el verbo rector y este se distingue de los demás que el legislador ha empleado, en que el primero es principal y los demás son accesorios.[48]

---

[46] Diariocritico.com, Computadores del 'Mono Jojoy': un motivo más de discordia**,** [en línea]. 2010. [consultado diciembre 1o. De 2020]. Disponible en: https://red.diariocritico.com/noticia/ 1466748/noticias/ computadores-del-mono-jojoy:-un-motivo-mas-de-discordia.html

[47] TOVAR, Carmen; Elementos del tipo Penal. [en línea]. 2010. [Consultado 1º. De abril de 2020[. Disponible en: edu/17110963/ Elementos_del_Tipo_Penal

[48] Ibid, p. 9

4.9.1.3 Bien Jurídico Tutelado (Objeto Jurídico)

Es el derecho que el legislador ha distinguido para resguardar mediante una norma penal; por ello se le denomina bien jurídico tutelado, protegido u objeto jurídico. Los bienes jurídicos son los valores ideales (inmateriales) de orden social sobre los que descansa la armonía, la paz social, y la seguridad de la vida en sociedad, El legislador elige determinado valor y al protegerlo mediante una norma penal, adquiere el nombre de bien jurídico penalmente protegido o tutelado [49].

4.9.1.4. Sujeto Activo

Es el autor, es decir; quien ejecuta la conducta, ya sea prohibitiva o imperativa indicada en la ley penal; se llama también, delincuente, agente o criminal. Este último concepto se emplea más desde el punto de vista de la criminología. Es útil afirmar, desde ahora, que el sujeto activo será siempre una persona física [50].

4.9.1.5 Sujeto Pasivo

Es el titular del bien jurídico, que ha sido afectado por la acción u omisión típica. Por lo general, se le señala también como víctima u ofendido, en cuyo caso una persona jurídica puede ser sujeto pasivo de un delito, como en los delitos patrimoniales y contra la Nación, entre otros [51].

4.9.1.6 Elemento Interno (Tipo Subjetivo)

Hace alusión a la función de la relación psicológica entre el autor y la acción o resultado, de donde se deriva el término DESVALOR DE ACCIÓN y se refiere a la finalidad, el ánimo, la tendencia que impulsó actuar al sujeto activo a realizar la acción y omisión, a título de dolo o de culpa. De este elemento se deriva el tipo doloso y el tipo culposo [52].

4.9.1.7 Elemento Material (Objeto Material)

El elemento u objeto material es la persona o cosa sobre la cual recae directamente el daño causado por el delito cometido. Cuando se trata de una persona, ésta se identifica con el sujeto pasivo, de modo que en una misma figura coinciden el sujeto

[49] Ibid, p. 11
[50] Ibid, p.11
[51] Ibid, p.12
[52] Ibid, p.14

pasivo y el elemento material; por tanto, la persona puede ser física o jurídica, por ejemplo, homicidio, lesiones y difamación. En estos delitos, el elemento material, que es la persona afectada, coincide con el sujeto pasivo del delito[53].

4.9.1.8 Conducta

Son las formas de comportamiento humano penalmente relevantes, que se ostentan en el mundo exterior tanto en acciones como en omisiones (propias o impropias). Ambas formas de comportamiento son relevantes para el Derecho Penal.

Figura 3. Elementos del tipo penal

Fuente: La autora

[53] Ibid, p.16

4.9.2 Los delitos tradicionales vinculados a la internet y los ciberdelitos. Si bien es cierto, los delitos vinculados a la internet se diferencian de los ciberdelitos por que los primeros protegen otros bienes jurídicos como el patrimonio, el buen nombre, la intimidad y no la información y los datos informáticos los cuales fueron protegidos por las Ley 1273 del 2009; para complementar la protección de estos bienes jurídicos de los posibles ataques producidos por medios informáticos, esta misma Ley en su artículo 2, adicionó un numeral 17 al artículo 58 del CP, por medio del cual se agrava la pena de los delitos no informáticos de la siguiente manera: "Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos"[54] agregándole mayor punibilidad a estos delitos; lo cual los coloca en desventaja con los delitos tradicionales dándoles un desvalor a la acción; esta condición debe ser tenida en cuenta por al momento de imponer la pena (CP, artículo 61; CPP, artículo 447).

4.9.3 Diferencias entre el Cibercrimen y los Delitos Comunes (así sean computacionales). Existen algunas diferencias entre la concepción de los Ciberdelitos y los delitos comunes así sean realizados por medios computacionales que tiene que ver especialmente de cómo se abordan, algunos elementos de tipo penal, los cuales serán descritos a continuación:

Tabla 6. Diferencias entre los ciberdelitos y los delitos comunes

Elementos del tipo penal	**Cibercrimen**	**Delitos Comunes (Computacionales)**
Bien Jurídico Protegido	Ley 1273 de 2009: protege de marea directa la seguridad de la información, los datos y el adecuado funcionamiento de los sistemas informáticos	Patrimonio, Buen nombre, intimidad….
Sujeto Activo	Usuario de un sistema informático o en calidad de ciberautor (cibernauta)	Una(s) persona(s) natural(es)
Elemento material u objeto sobre los cuales recae la acción	Los objetos digitales son al mismo tiempo medios virtuales (ámbitos)	Es el daño afecta directamente a una cosa, el objeto material será la

[54] POSADA-MAYA, Ricardo. El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad Virtual. [en línea]. 2017. [Consultado 3 de noviembre de 2020]. Disponible en: file:///C:/Users/MARTHA~1.GUA/AppData/Local/Temp/4751-Texto%20del%20art%C3%ADculo-17377-1-10-20170627.pdf

Elementos del tipo penal	Cibercrimen	Delitos Comunes (Computacionales)
	inherentes de ejecución del delito; que también son el objeto final sobre el que se ejecuta la acción cibercriminal. Ejm. Datos informáticos, La información, software, sistemas informáticos	cosa afectada por ejemplo: en el robo, la cosa mueble ajena es el objeto material; en el despojo lo son el inmueble, las aguas o los derechos reales; y en el daño en propiedad ajena lo son los muebles o los inmuebles.
Elemento subjetivo	Los cibercrímenes en Colombia conservan la estructura tradicional del dolo como conocimiento y voluntad (CP, artículo 22)67	Por ejemplo, el ánimo de lucro define el hurto, no basta solamente con apropiarse del bien, es necesario que haya ánimo de lucro para que sea considerado como doloso

FUENTE. La Autora, 2020

4.9.4 Metodología para identificar un Ciberdelito. Para identificar si una conducta inapropiada en el uso de los sistemas informáticos puede ser considerada como un delito informático o un Ciberdelito se deben seguir los pasos siguientes:

Paso 1. Confirmar la existencia de un *Supuesto Lógico.*

Para logar la tipificación de un Ciberdelito se debe partir del siguiente supuesto lógico:

la existencia de un sistema informático SI ☐ NO ☐

Paso 2. Identificar el *Verbo Rector*

Tomando la conducta inapropiada se debe analizar si encuadra en los siguientes verbos rectores:

Con respecto a los *Sistemas de Información:*

Acceder abusivamente SI ☐ NO ☐

Bloquear, obstruir, impedir ingreso SI ☐ NO ☐

Con respecto a los *Datos Informáticos y Programas:*

Interceptar, Impedir el ingreso SI ☐ NO ☐

Dañar, alterar, borrar, suprimir destruir SI ☐ NO ☐

Con respecto al uso *de Software Malicioso:*

Adquirir, distribuir, enviar, introducir SI ☐ NO ☐

Con respecto a *Datos Personales:*

Sustraer, vender, enviar, comprar, divulgar, emplear SI ☐ NO ☐

Con respecto a *Sitios Web:*

Suplantar SI ☐ NO ☐

Si en cualquiera de los casos la respuesta es SI, la conducta encuadra en un Ciberdelito.

Paso 3. Identificar el *Bien Jurídico:*

El bien Jurídico protegido por el legislador es:

La información y los Datos SI ☐ NO ☐

Paso 4. Identificar el *Sujeto Activo:*

Usuario de un sistema informático
o en calidad de ciberautor (cibernauta) SI ☐ NO ☐

Paso 4. Identificar el *Objeto Material*

Datos informáticos SI ☐ NO ☐

La información	SI		NO	
Software	SI		NO	
Sistemas informáticos	SI		NO	

Los elementos del tipo penal señalados anteriormente permiten identificar si la conducta inapropiada con respecto a los sistemas informáticos puede ser tipificada como un Ciberdelito de acuerdo con la Ley 1273 de 2009. Artículo 269 del Código Penal.

5. RESULTADOS

De acuerdo con lo definido en el documento, se establece que los delitos Informáticos son la agrupación de acciones u omisiones realizadas dentro del ciberespacio que promuevan un delito individual, social, económico, y/o político, contemplado en el orden jurídico territorial en el que se encuentre alguna de las partes implicadas (victima(s) y/o victimario(s)[55]. De igual forma se plantea que los Ciberdelitos son aquellas actividades delictivas o abusivas relacionadas con los ordenadores y las redes de comunicaciones, bien sea por utilizar el ordenador como herramienta del delito, o por que el objetivo del delito sea el sistema informático o la información allí contenida. De igual manera, Se definió que los ciberdelitos y los delitos informáticos están clasificados en tres grupos así: a) ciberdelitos o delitos informáticos con sentido económico, b) ciberdelitos o delitos informáticos sociales, y c). ciberdelitos políticos o ideológicos.

Para el desarrollo del presente documento se establecieron 4 Objetivos Específicos que permiten el cumplimiento del Objetivo General de los cuales se obtuvieron los siguientes resultados:

1. El Estado colombiano en el transcurso de los últimos 30 años ha emitido una serie de normas, que buscan confrontar los avances que ha tenido la tecnología con la aparición de una serie de conductas inapropiadas que se ejecutan utilizando estos medios tecnológicos. Esta normatividad tiene su inicio desde la expedición del Decreto 1360 de 1989; por el cual se reglamenta la Inscripción del Soporte Lógico (software) en el Registro Nacional del Derecho de Autor; hasta el Documento CONPES 3854 de 2016, que pretende diseñar una política pública de seguridad informática. En esta reglamentación tiene principal importancia la Ley 1273 de 2009, que adiciona el Articulo 269 del código Penal, ha marcado un hito en la legislación colombiana, porque ampara un bien jurídico intermedio no mencionado antes en las leyes y que tiene que ver con la protección de la información y de los datos. De igual manera, hace parte de los países del convenio de Budapest, Hungría a partir del 2018.

   Revisada la normatividad vigente en Colombia sobre delitos informáticos, para la identificación de conductas punibles que se ejecuten mediante la utilización de

[55] VALDERRAMA ESTUPIÑAN, Harrisson Jahir. El Papel de las Políticas y la Normatividad en la Prevención Y Regulación del Ciberdelito [en línea].2018 [consultado 1º. de abril de 2020]. Disponible en: (https://www. gestiopolis. com/ciberdelito-politicas-publicas-y-normatividad-para-su-prevencion-en-bogota-colombia/)

medios informáticos y se obtuvo lo siguiente: En el CPC en el artículo 269 A se tipifica el delito de acceso abusivo a sistemas informáticos y tiene como pena prisión de 48 a 96 meses y multa de 100 a 1.000 s.m.l.m.v; en el Artículo 269B, se establece el delito de Obstaculización ilegítima de sistema informático o red de Comunicaciones, con una pena de prisión de 48 a 96 meses y multa de 100 a 1. 000 s.m.l.m.v. En el Artículo 269C se tipifica el delito de Interceptación ilícita de datos informáticos y se le fija una pena de prisión de 36 a 72 meses. El artículo 269D se tipifica el delito de Daños informáticos, con una pena de prisión de 48 a 96 meses y multa de 100 a 1. 000 s.m.l.m.v Artículo 269E tipifica el delito de uso de software malicioso con una pena de prisión de 48 a 96 meses y multa de 100 a 1.000 s.m.l.m.v. El Artículo 269F Violación de datos personales con una pena de prisión de 48 a 96 meses y multa de 100 a 1.000 s.m.l.m.v. El artículo 269G tipifica el Delito de suplantación de sitios web para capturar datos personales e impone una pena de prisión de 48 a 96 meses y multa de 100 a 1.000 s.m.l.m.v. Igualmente, el artículo 218 del CPC tipifica el delito de Pornografía con menores de 18 años e impone una pena de prisión de 10 a 20 años y multa de 150 a 1500 s.m.l.m.v.

2. Las conductas delictivas cometidas mediante el uso de sistemas y/o medios electrónicos, no tipificados en la legislación colombiana como delitos informáticos, han sido para las personas un verdadero caos, pues siempre están tipificando como delitos informáticos a delitos tradicionales, solamente por la confusión entre delito y el medio o técnica empleada para su comisión. Dentro de los delitos tradicionales cometidos por medios electrónicos se encuentran: Ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas Art. 193 del CPC; Divulgación y empleo de documentos reservados, Art. 194 del CPC; la Violación ilícita de comunicaciones o correspondencia de carácter oficial, artículo 196 del CPC; Utilización ilícita de redes de comunicaciones, Art. 197 modificado ley 1453 de 2011; Violación a los derechos morales de autor, Art. 270 del CPC; la Violación de derechos patrimoniales de autor y derechos conexos Artículo 271 de CPC; y Violación a los mecanismos de protección de derechos de autor y derechos conexos y otras defraudaciones, Art. 272 del CPC.

El tratamiento jurídico e institucional y la interpretación de la norma ha sido circunstancias que inciden visiblemente en la definición de un delito informático, es allí donde se denota la falta de madurez en el tratamiento normativo penal de aquellas conductas que, no obstante, de ser antijurídicas y culpables, no son consideradas por el legislador como delitos informáticos es el caso de los ejemplos que se definen a continuación:

Tabla 7. Tratamiento dado por los jueces a conductas inapropiadas por medios informáticos

Medio	Delito que se le imputa
Clonación de Tarjetas	Violación de datos personales
Challenge o retos suicidas	Inducción o ayuda al suicidio
Utilización de Plataformas Webcam	Inducción a la prostitución
Ciber bullying	Injuria o Calumnia
Amenaza por medios electrónicos con fines lucrativos	Extorsión
Envío de correos electrónicos desde la cuenta de terceros	Violación de datos personales

Fuente: La Autora

3. De acuerdo con el informe presentado por el Tanque de Análisis y Creatividad de las TIC - TicTac de la CCIT y su programa SAFE en asocio con la Policía Nacional - Centro Cibernético Policial, en el "Tendencias del Cibercrimen 2019-2020", la denuncia de los delitos informáticos está en crecimiento, de acuerdo con la información suministrada por el aplicativo *ADenunciar,* la cual fue puesta en funcionamiento a partir de julio de 2017, en ese año se presentaron 15.844 casos, y para el año siguiente esta cifra se incrementó en un 41% (6.680) casos más que el año anterior 22.524 denuncias; para el año 2019 la cifra disminuyó a 15.948 denuncias este comportamiento es debido a que las entidades bancarias omitieron el requisito de la denuncia previa para las posibles reclamaciones.

   Desde la puesta en funcionamiento del aplicativo *ADenunciar* en el 2017, los colombianos han reportado 52.901 delitos informáticos, los cuales están distribuidos de la siguiente manera: del Delito Hurto por medios informáticos se han presentado 31.058 (59%) de denuncias; Acceso abusivo a sistemas informáticos 8.037 (15%) casos; Violación de datos personales 7.994 (15%) casos; Transferencia no consentida de activos 3.425 (6%), usos de software malicioso 2.383 (5%).

   De acuerdo con el Centro Cibernético Policial para el 2019, el 55% de los delitos informáticos ocurrieron en las siguientes ciudades: Bogotá 5.308 casos, Cali 1.190, Medellín 1.186, Barranquilla 643 y Bucaramanga 397. La ingeniería social es la causante de cerca del 90% de los ciberataques perpetrados a las empresas que funcionan en Colombia. De acuerdo con la modalidad de intrusión, los ataques BEC, lideran las denuncias recibidas por las autoridades de las diferentes estafas, las principales son las siguientes: Correos Fraudulentos Personalizados (Spear

Phishing); Suplantación de identidad; Enmascaramiento de correos (Spoofing); Infección de sitios frecuentemente visitados por empleados (Watering Hole)[56], seguido de los Ransomware presentándose en Colombia el 30% de los ataques en Latinoamérica; los Ataques de Denegación del servicio fueron reportados por 170 empresas quienes denunciaron interrupciones en el servicio de cara a los clientes; los Malware o software malicioso se incrementaron con respecto al año anterior en un 612%, al pasar de 99 casos reportados en el 2018 a 705 en el 2019, siendo las PYME las más afectadas; otra modalidad que está comenzando a tener auge dentro de los ciberdelincuentes es la minería de criptomonedas.

Las recomendaciones más importantes para evitar ser víctima de un delito informático para empresas que puede ser aplicadas para personas son las siguientes:

- Para las empresas que no tengan definida e implementada un Sistema de Gestión de Seguridad de la Información –SGSI, pueden implantar las normas ISO/IEC 27001 e ISO/IEC 27701 paralelamente.
- Evitar realizar tareas sensibles para la organización desde el teléfono celular, como el uso de correo electrónico corporativo, porque puede perderse información valiosa para la compañía.
- Se debe implementar una adecuada política de almacenamiento de información en la nube, definiendo el tipo de información y el tiempo de permanencia en los repositorios virtuales.
- Se debe definir el uso del correo corporativo, para actividades estrictamente empresariales, evitando circular aplicaciones de juegos, ocio o citas.
- Guardar una regulación directa en la política de proveedores y clientes; como también del manejo de estos con la ciberseguridad de la empresa.
- Es muy importante establecer mecanismos perimetrales de protección como antivirus, antimalware, anti-fishing indispensables en la infraestructura del negocio.
- Si la empresa ha sido víctima de algún ataque debe desarrollar la capacidad de ciberresiliencia aplicándola en las tres áreas críticas: seguridad de la información, la continuidad del negocio y la capacidad de recuperación de la organización.
- Si la empresa aún no ha sido víctima de ningún ataque, debe prepararse para afrontar este tipo de situaciones, definiendo cuales son los roles y responsabilidades que tiene cada uno de los actores involucrados en el plan de respuesta y gestión de un incidente cibernético.

[56] TOVAR, Carmen; Elementos del tipo Penal. {en línea}. 2010. {Consultado 1º. De abril de 2020}. Disponible en: edu/17110963/ Elementos_del_Tipo_Penal

4. Para identificar si una conducta inapropiada es considerada como delito informático, se requiere cotejarla y tipificarla, para tal fin, se debe revisar el cumplimiento de unos requisitos denominados Elementos del Tipo Penal, los cuales están definidos por el Código penal y son los siguientes:

   Se debe partir de un *Supuesto Lógico* este es un presupuesto totalmente necesario para demostrar la existencia de un delito; un *Verbo Rector* es un verbo en forma infinitiva principal sobre la cual se desarrolla la conducta*; Bien Jurídico* son los valores ideales (inmateriales) de orden social sobre los que descansa la armonía, la paz social, y la seguridad de la vida en sociedad, estos son determinados por el legislador; Sujeto Activo, es el autor o quien realiza la conducta*; Sujeto Pasivo* es el titular del bien jurídico; *Elemento Subjetivo* es la finalidad que tuvo al actuar el sujeto activo; *Elemento Material* persona o cosa sobre la cual recae el daño causado.

   Para identificación de los delitos informáticos se propuso una metodología sencilla donde se aborda cada uno de los elementos del tipo penal que deben hacer parte de en la identificación y tipificación de un delito.

   De acuerdo con el análisis realizado en la presente monografía, actualmente Colombia cuenta con suficientes elementos normativos que permiten a los jueces sancionar y penalizar las conductas ilícitas considerados como Delitos Informáticos; sin embargo, hay que tener en cuenta que existe una desinformación frente a la forma de abordar los comportamientos no todas las conductas inapropiadas realizadas mediante el uso de medios informáticos son ciberdelitos, por esta razón, es importante saber distinguir entre un delito común cometido a través de medios informáticos y un verdadero Ciberdelito, esto es uno de los objetivos específicos planteados y desarrollado en el documento.

6. CONCLUSIONES

- Al momento de establecer si una conducta inapropiada es un delito, lo primero a tener en cuenta, es que la legislación tiene dentro de sus principios básicos el *Principio de Legalidad,* que establece que nadie podrá ser juzgado sino conforme a las leyes preexistentes al acto que se le imputa. Esta norma quiere decir, que si la conducta no se encuentra descrita "exactamente dentro de un tipo penal especifico", no podrá ser juzgada por el ordenamiento penal[57]. Es importante aclarar que no siempre que una conducta parezca delincuencial, es un delito; solamente es considerada delito, aquella que ha sido tipificada como tal, por el legislador.

- Los delitos Informáticos son una agrupación de acciones u omisiones cometidas dentro del ciberespacio que promuevan un delito individual, social, económico, y/o político, contemplado en el orden jurídico territorial en el que se encuentre alguna de las partes implicadas víctima(s) y/o victimario(s)[58]. Los Ciberdelitos son aquellas actividades delictivas o abusivas relacionadas con los ordenadores y las redes de comunicaciones, bien sea por utilizar el ordenador como herramienta del delito, o por que el objetivo del delito sea el sistema informático o la información allí contenida. De igual forma, los delitos informáticos están clasificados en tres grupos así: A. delitos informáticos con sentido económico, B. delitos informáticos sociales, y C. políticos o ideológicos[59].

- La Ley 1273 de 2009, crea un nuevo *bien jurídico intermedio* que tutela el concepto de la *protección de la información y de los datos*, tipificando en Colombia los delitos informáticos así: acceso abusivo a un sistema informático (modificado del Código Penal); obstaculización ilegítima del sistema informático o red de telecomunicación;

---

[57] GUZMAN A. Clara L. Contextualización del cibercrimen en Colombia, 11 (28): 41-66 Vol. 4 Núm. 7, 2009. [consultado 15 de abril de 2020], [en línea], Disponible https://studylib.es/doc/8020365/descargar-el-archivo-pdf

[58] VALDERRAMA ESTUPIÑAN, Harrisson Jahir. El Papel de las Políticas y la Normatividad en la Prevención Y Regulación del Ciberdelito [en línea].2018 [consultado 1º. de abril de 2020]. Disponible en: (https://www. gestiopolis. com/ciberdelito-politicas-publicas-y-normatividad-para-su-prevencion-en-bogota-colombia/)

[59] OJEDA-PEREZ, Jorge Eliécer; RINCON-RODRIGUEZ, Fernando; ARIAS-FLOREZ, Miguel Eugenio and DAZA-MARTINEZ, Libardo Alberto. Delitos informáticos y entorno jurídico vigente en Colombia. Cuad. Contab. vol.11, n.28,. [en línea]. 2010.[consultado 15 de mayo de 2020]. Disponible en: https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

interceptación de datos informáticos; daño informático; uso de software malicioso; hurto por medios informáticos y semejantes; violación de datos personales; suplantación de sitios *web* para capturar datos personales y transferencia no consentida de activos.[60]

- El ordenamiento jurídico vigente en Colombia se ha convertido en una importante contribución para enfrentar "los delitos informáticos", ya que contiene definidas políticas de seguridad de la información, algunos procedimientos y detalladas las acciones penales que se pueden adelantar en contra de las personas que incurran en este tipo de conductas.

- Los delitos vinculados a la internet se diferencian de los ciberdelitos por que los primeros protegen otros bienes jurídicos como el patrimonio, el buen nombre, la intimidad y no la información y los datos informáticos los cuales fueron protegidos por la Ley 1273 del 2009; para complementar la protección de estos bienes jurídicos de los posibles ataques producidos por medios informáticos, esta misma Ley en su artículo 2, adicionó un numeral 17 al artículo 58 del CP, por medio del cual se agrava la pena de los delitos no informáticos de la siguiente manera: "Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos"[61]

- Entre las principales modalidades de ataques BEC se encuentran las siguientes: *Estafa de CEO o suplantación del Gerente:* esto sucede mediante correo malicioso que se apodera de la cuenta de correo del gerente se envían correos a los empleados encargados de realizar los pagos y dispensar los fondos y así realizar las transferencias a las cuentas falsas. *Suplantación de clientes:* mediante correos engañosos se realizan los cobros de facturas y el recaudo se hace en las cuentas de los *mone*, que son personas que prestan sus cuentas para que se cometan estos tipos de delitos.

- Es el derecho que el legislador ha seleccionado para protegerlo mediante una norma penal; por ello se le denomina bien jurídico tutelado, protegido u objeto jurídico. Los bienes jurídicos son los valores ideales (inmateriales) de orden social sobre los que descansa la armonía, la paz social, y la seguridad de la vida en

---

[60] CONGRESO DE LA REPÚBLICA, CODIGO PENAL COLOMBIANO, Ley 599 de 2000. [en línea]. 2000. [consultado 13 de abril de 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html

[61] POSADA-MAYA, Ricardo. El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad Virtual. [en línea]. 2017. [Consultado 3 de noviembre de 2020]. Disponible en: file:///C:/Users/MARTHA~1.GUA/AppData/Local/Temp/4751-Texto%20del%20art%C3%ADculo-17377-1-10-20170627.pdf

sociedad, El legislador elige determinado valor y al protegerlo mediante una norma penal, adquiere el nombre de bien jurídico penalmente protegido o tutelado [62].

[62] TOVAR, Carmen; Elementos del tipo Penal. [en línea]. 2010. [Consultado 1º. De abril de 2020]}. Disponible en: edu/17110963/ Elementos_del_Tipo_Penal

7. RECOMENDACIONES

- El conocimiento de la normatividad existente para el tratamiento de delitos informáticos no es responsabilidad de los abogados solamente, en razón a que todas las profesiones aplican dentro de su desarrollo y quehacer cotidiano, tecnologías informáticas y pueden ser sujetas a cualquier tipo de conducta delictiva; por tal razón, es necesario que las universidades incluyan dentro de su pensum académico de todas la carreras, Derecho Informático y seguridad informática, aplicados al programa específico.

- Los funcionarios que imparten justicia deben ser capacitados en seguridad informática y en la aplicación del Derecho informático al tratamiento de delitos informáticos de acuerdo con la normatividad vigente en Colombia, con el fin de unificar criterios sobre el análisis jurídico necesario para la aplicación de la norma, la tipificación de las conductas y la aplicación de la pena y así evitar que cada uno de los fallos deban ser objetados ante la Corte Suprema de Justicia

- Se deben promover campañas de divulgación para la prevención de los delitos informáticos para que las personas protejan de manera adecuada la información y los datos como los demás bienes jurídicos que pueden llegar a ser sujetos de ataques por medios informáticos.

- Según los reportes de las autoridades las pequeñas y medianas empresas PIME, son las mayores víctimas de todo tipo de ataque informático, por tal razón, de debe buscar del Estado mecanismos de protección para estas empresas pues según la información disponible, éstas no logran sobrevivir a un ataque informático.

REFERENCIAS BIBLIOGRÁFICAS

ALCURIO DEL PINO, Santiago. Delitos informáticos. [en línea]. 2014. [consultado 17 de mayo de 2020]. Disponible en: https://www.oas.org/juridico /spanish/cyb_ecu_delitos_inform.pdf

ALVAREZ MARAÑON, Gonzalo y PEREZ GARCIA PEDRO, Seguridad Informática para la empresa y particulares, [en línea]. 2004. [consultado 17 de mayo de 2020]. Disponible en: https://editorial.tirant.com/es/libro/seguridad-informatica-para-empresas-y-particulares-9788448140083

BAÓN RAMÍREZ, Rogelio. Visión general de la informática en el nuevo Código Penal, en Ámbito jurídico de las tecnologías de la información, Cuadernos de Derecho Judicial, Escuela Judicial/Consejo General del Poder Judicial, Madrid, [en línea]. 1996. [consultado 17 de mayo 2020]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=552416

Bienes Jurídicos intermedios: Son aquéllos cuya tutela va dirigida a evitar la lesión mediata o inmediata de otros bienes jurídicos [en línea] 1999. [consultado septiembre 12 de 2020]. Disponible en: https://sites.google.com/site/josycordova 7/15-bien-juridico-datos-e-intimidad-personal/14-5-bien-juridico-individual-y-colectivo

CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES, Informe sobre el Ciberdelito en Colombia, [en línea]. 2017 [consultado el 1º. De abril de 2020]. Disponible en: https://www.infolaft.com/la-camara-colombiana-de-informatica-y-telecomunicaciones-lanza-informe-sobre-cibercrimen/

CASTRO MUÑOZ, Juan José, La imputación Objetiva [en Línea] 2016, [consultado 25 de agosto de 2020]. Disponible en: https://www.asuntoslegales.com.co/analisis/juan-jose-castro-munoz-530496/la-imputacion-objetiva-2444266

COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley 44 de 1993. [en línea]. 1993. [consultado 1º. De abril de 2020] Disponible en: https://propiedadintelectual.unal.edu.co/fileadmin/recursos/innovacion/docs/normatividad_pi/ley44_1993.pdf

COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley 599 de 2000. Código Penal Colombiano. [en línea]. 2000. [consultado el 1º. de abril de 2020]. Disponible en: https://co.biblioteca.legal/codigo-penal/violacion-intimidad-interceptacion-comunicaciones

COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley 1273 de 2009. [en línea]. 2009. [consultado el 1º. de abril de 2020]. Disponible en: https://www.oas.org/dil/esp/LEY_1336_DE_2009_Colombia.pdf

COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley 1336 de 2009, [en línea]. 2009. [consultado 1º. De abril de 2020]. Disponible en: https://diario-oficial. vlex. com.co/vid/robustece-pornografia-adolescentes-61325313

COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley 1341 de 2009, [en línea]. 2009. [consultado 1º. De abril de 2020]. Disponible en: https://www. mintic. gov. co/portal/inicio/3707: Ley-1341-de-2009

COLOMBIA, CONGRESO DE LA REPÚBLICA, Ley 1581 de 2012, [en línea]. 2012. [consultado 1º. De abril de 2020] Disponible en: http://www. secretariasenado. gov. co/senado/basedoc/ley_1581_2012.html

COLOMBIA. CORTE SUPREMA DE JUSTICIA, Sala de Casación Penal, [en línea]. 2010. [consultado diciembre 1o. De 2020]. Disponible en: https://es.slideshare.net/Alediaganet/sentencia-34564-25-08-10-competencia-transferencia-activos

COLOMBIA, FISCALÍA GENERAL DE LA NACIÓN, Proceso de Investigación y judicialización. [en línea]. 2015. [consultado diciembre 1o. De 2020]. Disponible en: https://www.fiscalia.gov.co/colombia/wp-content/uploads/20170111.pdf

CULPABILIDAD [Anónimo]. [en línea]. 2003. [consultado 15 de mayo de 2020]. Disponible en: https://www.ecured. cu/Culpabilidad

DEPARTAMENTO NACIONAL DE PLANEACIÓN -DNP. Documento CONPES 3701 de 2011 [en línea] 2011. [consultado 15 de mayo de 2020]. Disponible en: https://www.mintic.gov..co /portal/604/articles-3510_documento.pdf

DEPARTAMENTO NACIONAL DE PLANEACIÓN – DNP, Documento CONPES 3854. [en línea]. 2008. [Consultado 1º. De abril de 2020]. Disponible en: (https://colaboracion. dnp. gov. co/CDT/ConpesEcon% C3%B3micos/3854_Adenda1. pdf)

DIARIOCRITICO.COM, Computadores del 'Mono Jojoy': un motivo más de discordia**,** [en línea]. 2010. [consultado diciembre 1o. De 2020]. Disponible en: https://red.diariocritico.com/noticia/ 1466748/noticias/ computadores-del-mono-jojoy:-un-motivo-mas-de-discordia.html

EL BIEN JURÍDICO EN EL DERECHO PENAL, [en línea] 2018. [consultado el 15 de mayo de 2020]. Disponible en: https://www.palladinopellonabogados.com/el-bien-juridico-en-el-derecho-penal/

EL TIEMPO, En el 2019 se reportaron más de 28.000 ciberataques en Colombia, [en línea]. 2019 [consultado 15 de mayo de 2020]. Disponible en: https://www.eltiempo.com/tecnosfera/novedades-ecnologia/reporte-de-ciberataques-en-colombia-2019-de-policia-nacional-y-ccit-428790

GÓMEZ PERALS, Miguel, Los Delitos Informáticos en el Derecho Español. [en línea]. 2003. [consultado 15 de mayo de 2020]. Disponible en: https//Dialnet-LosDelitosInformaticosEnElDerechoEspanol-51084%20(1).pdf

GUZMAN A. Clara L. Contextualización del cibercrimen en Colombia, 11 (28): 41-66 Vol. 4 Núm. 7, [en línea] 2009. [consultado 15 de abril de 2020], Disponible en: https://studylib. es/doc/8020365/descargar-el-archivo-pdf

GUTIÉRREZ GÓMEZ, María Clara. Consideraciones sobre el tratamiento jurídico del comercio electrónico. En: Internet, comercio electrónico y comunicaciones. [en línea].2004. [consultado 9 abril de 2020]. Disponible en: http://www.scielo.org.co/scielo.php?script=sci_nlinks&ref=000247&pid=S0041-060201500020000800008&lng=en

INTERPOL. Lista Información de seguridad y prevención de la delincuencia de la empresa. [en línea]. 2010 [consultado 1º. De abril de 2020]. Disponible en: http://www. interpol. int/Public/TechnologyCrime/CrimePrev/companyChecklist. asp#top. Recuperado el 28 de enero de 2010

MAYER LUX, Laura; EL BIEN JURÍDICO PROTEGIDO EN LOS DELITOS INFORMÁTICOS, [en línea] 2017 [consultado el 15 de mayo de 2020]. Disponible en: https://scielo.conicyt.cl /scielo.php?script= sci_arttext&pid=S0718-34372017000100011

OJEDA-PEREZ, Jorge Eliécer; RINCON-RODRIGUEZ, Fernando; ARIAS-FLOREZ, Miguel Eugenio and DAZA-MARTINEZ, Libardo Alberto. Delitos informáticos y entorno jurídico vigente en Colombia. Cuad. Contab. vol.11, n.28, [en línea].2010. [consultado 15 de mayo de 2020]. Disponible en: https://www.mintic.gov.co/portal/604/articles-3510_documento.pdf

OSORIO MORENO, César Alejandro. Evolución de la protección penal del Derecho de Autor en Colombia. [en línea]. 2010 [consultado en noviembre 1º. de 2020]. Disponible en: http://www.scielo.org.co/ scielo.php?script =sci_arttext&pid=S0121-86972010000200007

PEREZ PORTO, Julián; MERINO, María, Definición de Tipicidad. [en línea]. 2016. [Consultado 15 de abril de 2020]. Disponible en: https://definicion. de/tipicidad/

PEÑA VALENCIA, Juliana, Legislación aplicable a las conductas delictivas en internet, [en línea]. 2010. [Consultado 1º. De abril de 2020]. Disponible en (http://bibliotecadigital. usbcali. edu. co/bitstream/ 10819/737/1/Legislacion_ Aplicable_Conductas_Pena_2009. pdf)

PINO, Francisca. Antijuricidad en el Derecho Penal, Apuntes de Derecho Penal, [en línea]. 2019. [Consultado 15 de abril de 2020]. Disponible en: https://definicion. de/tipicidad/https://www. docsity. com/es/antijuricidad-en-el-derecho-penal/4522972

POSADA MAYA, Ricardo, Una Aproximación a la Criminalidad informática en Colombia, 2017. en Revista de Nuevo Foro Penal No. 88, enero-junio 2017, Universidad EAFIT

POSADA-MAYA, Ricardo. El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad Virtual. [en línea]. 2017. [Consultado 3 de noviembre de 2020]. Disponible en: file:///C:/Users/MARTHA~1.GUA/AppData/Local/Temp/4751-Texto%20del%20art%C3%ADculo-17377-1-10-20170627.pdf

REVISTA AMBITO JURÍDICO, Las insólitas condenas por el mal uso de las redes sociales [en línea] 2017 [Consultado diciembre 3 de 2020]. Disponible en: https://www.ambitojuridico. com/noticias/tic/las-insolitas-condenas-por-el-mal-uso-de-las-redes-sociales

REVISTA SEMANA, CIBERCRIMEN, El 'rey millas' que le dio la vuelta al mundo a cuenta de Sofía Vergara, Juanes y otros famosos. [en línea] 2018 [Consultado diciembre 3 de 2020]. Disponible en: emana.com/tecnologia/articulo/jaime-alejandro-solano-moreno-el-rey-millas-que-viajo-por-cuenta-de-sofia-vergara-juanes-y-otros-famosos/561833/

SUÁREZ SÁNCHEZ, Alberto. La estafa informática [en línea]. 2009. [Consultado 1º. de abril de 2020]. Disponible en: (https://delitosinformaticos. com/tag/estafa-informatica)

TANQUE DE ANÁLISIS Y CREATIVIDAD DE LAS TIC - TICTAC DE LA CCIT, El estudio Tendencias del Cibercrimen 2019-2020. [en línea]. 2020. [Consultado 3 de

noviembre de 2020]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

TOVAR, Carmen; Elementos del tipo Penal. [en línea]. 2010. [Consultado 1º. De abril de 2020[. Disponible en: edu/17110963/ Elementos_del_Tipo_Penal

VALDERRAMA ESTUPIÑAN, Harrisson Jahir. El Papel de las Políticas y la Normatividad en la Prevención Y Regulación del Ciberdelito [en línea]. 2018 [consultado 1º. de abril de 2020]. Disponible en: (https://www. gestiopolis. com/ciberdelito-politicas-publicas-y-normatividad-para-su-prevencion-en-bogota-colombia/

VARGAS ARCINIEGAS, Cristhian Francisco La regulación del “Grooming” o ciberacoso infantil desde una perspectiva comparada: un análisis de las legislaciones de Argentina, México y Colombia [en línea]. 2008. [Consultado 1º. De abril de 2020]. Disponible en: https://ciencia. lasalle. edu. co/cgi/viewcontent. cgi?article=1095 &context=negocios_relaciones