EL CIBERDELITO: UN NECESARIO AGRAVANTE DE LA ESTAFA EN EL CÓDIGO PENAL COLOMBIANO

JORGE GÓMEZ FONSECA

Universidad la Gran Colombia

Maestría en Derecho

Bogotá, D.C., 2023

EL CIBERDELITO: UN NECESARIO AGRAVANTE DE LA ESTAFA EN EL CÓDIGO PENAL COLOMBIANO

JORGE GÓMEZ FONSECA

Trabajo de Grado presentado como requisito para optar al título de Magister en Derecho

PhD VICTOR MANUEL CACERES TOVAR

Universidad la Gran Colombia

Maestría en Derecho

Bogotá, D.C., 2023

Dedicatoria

Dedico con todo mi corazón esta tesis a mi amada esposa y a mis hermosas y bellas hijas, a las que amo con todo mi corazón, ya que son ellas quienes han creído y contribuido en todo momento, para así poder conseguir este nuevo logro en mi vida personal y profesional, personas que por siempre voy a tener en mi corazón y ruego a Dios siempre estén en mi vida.

Ellas con su dedicación, empeño y paciencia, me permitieron avanzar en cada uno de los capítulos de este trabajo, el cual, sin duda se constituye no solo en un logro personal sino familiar en el cada hoja contiene algo de ellas, sin ustedes, habría sido imposible alcanzar éste tan anhelado peldaño.

También a mi familia, que siempre ha estado ahí acompañándome en todos y cada uno de los momentos de mi vida, nunca me han dejado solo, mis amadas hermanas Olga y Yaneth forjadoras de este hombre que soy, con las siempre estaré en deuda y quienes sin duda, al igual que yo, disfrutaremos de las consecuencias positivas de esta investigación.

Agradecimientos

Agradecido siempre con Dios por permitirme llegar a este nuevo logro, quien ha estado conmigo en cada momento, colocando en mi camino a todas y cada una de aquellas personas que de una u otra manera han aportado cosas importantes en mi carrera.

Mi profundo y mis más sincero agradecimiento al Doctor Víctor Manuel Cáceres, educador del más alto nivel, quien, con cada una de sus observaciones, indicaciones y acompañamientos, me permitió la construcción de este, que considero, mi mayor logro profesional.

Al Doctor Javier Vera, por su guía y orientación incondicional, para él mi más grande admiración y respeto.

De igual forma un especial y fuerte agradecimiento a la Universidad Gran Colombia, a la facultad de Derecho, por recibirme y permitir este avance profesional.

Tabla de contenido

Glosario

Cibercrimen: Es un tipo de actividad delictiva, el cual se lleva cabo a través de un dispositivo electrónico como lo es, una computadora o un celular que se encuentra conectado en la red y de manera ilegal obtiene información personal y privada.

Cibercriminal: Persona que utiliza la internet para cometer hechos delictivos.

Estafa: Delito que se encuentra regulado por nuestro Código Penal (2000) en el artículo 246, en cuyo contenido manifiesta:

> El que obtenga provecho ilícito para sí o para un tercero, con perjuicio ajeno, induciendo o manteniendo a otro en error por medio de artificios o engaños, incurrirá en prisión de 2 a 8 años y multa de 50 a mil 1000 salarios.

Hacker: Persona con avanzados conocimientos sobre informática, que le permite ingresar de manera ilegal a diferentes sistemas tecnológicos y obtener de ellos la mayor información posible, para de esta manera poder cometer ilícitos.

Piratas informáticos: Es la persona que accede de manera ilegal a un sistema informático en busca de apropiarse de información secreta de personas naturales o jurídicas, cuyo único propósito es el de lucrarse al vender de manera masiva sus contenidos.

Resumen

La revolución informática nacida con el nuevo siglo llevada hasta la actualidad nos ha traído una gran cantidad de beneficios y comodidades para el normal desarrollo cotidiano de nuestras vidas, pero con ellas, también han llegado un sin número de nuevos delitos que se han ido implementando por personas que ven en los medios electrónicos un mecanismo necesario en nuestro diario vivir. Siendo así, y teniendo en cuenta que los nuevos delitos informáticos y los ciberdelincuentes son una nueva generación de autores y conductas, se requiere, a través de nuevas herramientas, investigar y analizar desde diversas ópticas la problemática, para poder contrarrestar este creciente flagelo. Existe, en este contexto, una falencia que viene a estar orientada en la aplicación normativa y por supuesto inexistencia de jurisprudencia reciente, ya que la misma no se actualiza de manera constante y ha dejado algunos vacíos que no han permitido estar en la misma carrera de los delincuentes y su modus operandi.

La necesidad surge de la construcción de un sistema penal mucho más robusto, que entiende las nuevas formas delictivas a efectos de hacer muchos más eficiente nuestro sistema acusatorio, en la búsqueda y actualización de conocimientos, con la promulgación de nuevos instrumentos que permitan enfrentar de la mejor manera, todo el andamiaje criminal de manera directa y objetiva en el momento en que se presente la comisión de un delito que involucre medios tecnológicos en su realización.

Abstract

The computer revolution born with the new century carried on to the present day has brought us a large number of benefits and comforts for the normal daily development of our lives, but with them, a number of new crimes have also come that have been implemented by people who see electronic media as a necessary mechanism in our daily lives. Thus, and taking into account that new computer crimes and cybercriminals are a new generation of perpetrators and behaviors, it is required, through new tools, to investigate and analyze the problem from different perspectives, in order to counteract this growing scourge. There is, in this context, a flaw that comes to be oriented in the normative application and of course the inexistence of recent jurisprudence, since it is not constantly updated and has left some gaps that have not allowed to be in the same career of criminals and their modus operandi.

The need arises from the construction of a much more robust criminal system, which understands the new criminal forms in order to make our accusatory system much more efficient, in the search and updating of knowledge, with the promulgation of new instruments that allow us to face the better way, all the criminal scaffolding in a direct and objective way at the moment in which the commission of a crime that involves technological means in its realization occurs.

Keywords: Cybercrime, cybercriminals, hackers, swindle,

Introducción

La presente investigación tiene como referencia a los delitos informáticos en Colombia y sus diferentes modalidades, las cuales son utilizadas por el crimen organizado en la actualidad, que según estadísticas presentadas por la Policía Nacional en su reporte anual para el año 2019 en la revista de criminalidad, determinó que el delito informático aumento en un 54% con respecto al año 2018, debido a que un gran número de personas en la actualidad utilizan las plataformas electrónicas para realizar toda clase de transacciones comerciales.

Los ciberdelincuentes están en constante modificación de su modus operandi para de esta manera poder estar a la vanguardia y poder romper los bloqueos de seguridad que son actualizados también a diario. Si bien, los ciberpiratas nos muestran nuevas modalidades para delinquir, también lo es, que las autoridades han creado la necesidad de mantener un constante cambio frente a la forma de obtener las mejores herramientas y poder contrarrestar el accionar de estos sujetos delictivos.

Se requiere, de acuerdo con estos nuevos sistemas delictivos, elementos de lucha, los cuales pueden verse reflejados en el fortalecimiento de nuestro Código Penal y su consecuente desarrollo a través de decretos que permitan el fortalecimiento de nuestra legislación en materia penal, para de esta manera poder llevar ante los estrados judiciales a las personas que están detrás de estos ataques como se pretende demostrar en este caso en particular relacionado con la estafa cometida por medios tecnológicos y cuya falencia encuentra gran calado en la falta de la materialización de un agravante para este tipo de actuación criminal. La necesidad es imperiosa, teniendo en cuenta que es uno de los delitos más comunes ya que son cometidos utilizando la internet, sin que en muchas ocasiones las personas se lleguen a dar cuenta de quién o de qué manera fueron estafados.

La Policía Nacional y la Fiscalía General de la Nación, en sus diferentes pronunciamientos ante los medios de comunicación (radio y televisión) además de las redes sociales y las diferentes plataformas de internet, muestran a diario un acontecer creciente de esta clase de delitos informáticos, los cuales, en nuestros días, es de un constante trasegar por la fácil inmersión de la información personal e industrial a los medios electrónicos.

Los ciberdelincuentes operan desde plataformas tecnológicas que en ocasiones son difíciles de rastrear por las autoridades, lo que ha hecho que este delito sea una nueva especialización criminal llevando su actuar a un nuevo comportamiento delictivo en el ámbito informático, esto, debido a una proliferación de conductas antisociales de nuestros nuevos hábitos de vida en la internet, la muy cambiante y constante actualización de nuestra información electrónica en la diferentes plataformas electrónicas que ha permitido que los ciberdelincuentes tengan acceso mucho más fácil a la comisión de este delito de la ciber estafa y el acceso a este medio delictivo a través de la internet sin que se encuentre un medio eficaz de poder rastrear y contrarrestar de manera efectiva a las personas o grupos que tienen como actividad económica este fraude cibernético como la estafa por medios tecnológicos.

La problemática social a la cual nos enfrentamos con estos Ciberdelitos ha creado la necesidad de estudiar a fondo cuales son los diferentes artículos de nuestro Código Penal Colombiano que necesitan ser robustecidos, para así y de esta manera poder contrarrestar el delito de la estafa por medios tecnológicos y que sean mucho más aplicables a estos fenómenos. Es de vital importancia, a la par de fortalecer nuestro sistema, buscar herramientas que nos permitan establecer cuáles son los métodos más utilizados por los ciber delincuentes para la comisión de estos delitos informáticos y tratar de articular de una manera adecuada con los operadores judiciales de la comunidad internación para buscar desde diversos puntos la mejor manera de

enfrentar este tipo de flagelos. Para ello, y simplemente para poner en contexto la investigación, se hizo un análisis del sistema judicial Español, en el que se presenta un más completo aparato judicial que permite impartir justicia de manera más eficaz cuando se presentan este tipo de conductas.

En esa búsqueda de como poder aplicar esta reforma a la legislación penal, permite ver la necesidad de que sea modificado el artículo 247 del Código Penal Colombiano el cual contiene los agravantes de la estafa y que allí sea incluido el realizado por medios tecnológicos y utilizando la internet para cometer el delito, para que de esta manera la aplicabilidad en el momento de imponer condena se haga de manera directa, utilizando, de ser necesario, la Ley 1273 del 2009 como soporte principal al agravante de la estafa cometido por medio tecnológico.

Desde la creación de la Ley 1273 de 2009 la legislación Colombiana debió haber realizado cambios dentro de los agravantes de la estafa en su artículo 247 del Código Penal, para que de esta manera su aplicabilidad fuese más directa y no utilizar solamente la Ley 1237 de 2009 para el proceso de judicialización para todos los delitos cibernéticos en general, ya que uno de ellos necesita un manejo del proceso judicial completamente diferente a los demás Ciberdelitos, apoyados en la Ley 906 de 2004 y de claridad procedimental al Código Penal, para que así de esta manera sea más entendible el tipo de conducta infringida y las circunstancias en las que se cometió dicha conducta en la modernización del mismo delito, entendiendo la forma y el fondo de operar de los ciberdelincuentes.

La metodología de investigación utilizada para este trabajo de grado está basada en la recolección de datos para probar la hipótesis basada en análisis para establecer patrones de comportamiento estadístico propuesto por Sampieri (2004) en su libro la metodología de la investigación el cual nos narra que:

> La investigación puede cumplir dos propósitos fundamentales: a) producir conocimiento y teorías (investigación básica) y b) resolver problemas prácticos (investigación aplicada). Gracias a estos dos tipos de investigación la humanidad ha evolucionado. La investigación es la herramienta para conocer lo que nos rodea y su carácter es universal. (p. 1)

A su turno Narváez, indica que "La recolección de la información se basa en un conjunto de procesos sistemáticos y empíricos que se aplica al estudio de un fenómeno". (p. 2) El tipo de investigación básica, que se realiza con la recopilación de conocimientos y teorías ya realizadas, para de esta manera robustecer la metodología de la investigación, se soporta en el libro de metodología de la investigación de Sampieri, en sus artículos tercero, cuarto y quinto, donde nos habla claramente del método de recolección de información de manera primaria la cual se fundamenta, el cómo nos lo plantea en el capítulo quinto de su libro, que trata sobre el proceso sistemático y empírico que se aplica al estudio de un fenómeno en especial como el que nos atañe en este caso como lo es la estafa cometida por medios tecnológicos.

Se hace necesario recopilar información de las investigaciones ya realizadas, leyes, Decretos y toda clase de jurisprudencia emitidita por las altas Cortes como lo es el Consejo de Estado, Congreso de la República desde el año 2015 hasta el primer semestre del año 2020 para poder llegar a concluir que toda esta información recolectada nos hace ver la necesidad de modificar el artículo 247 el cual nos habla sobre los agravantes de la estafa, la investigación fundamental busca el conocimiento de la realidad o de los fenómenos que allí converjan, para contribuir a una sociedad cada vez más avanzada y que responda mejor a los retos que ella demanda, teniendo en cuenta que en la legislación colombiana no se encuentra como agravante de la estafa aquellos cometidos por medios tecnológicos ya que son muy pocos los pronunciamientos realizados.

Para llevar a cabo esta metodología de investigación se realizara una búsqueda exhaustiva de información existente a nivel nacional e internacional sobre las normas, leyes, estadísticas de las entidades del Estado como lo es la Policía Nacional y la Fiscalía General de la Nación e investigaciones previas ya realizadas sobre el ciber delito, además de la información jurídica existente hasta el primer semestre del año 2020 sobre la aplicación de la norma en contra del ciber delito, además de todo lo que tenga relación con la parte jurídica y derecho comparado, con el fin de hacer una recopilación teórica para ser contrastada empíricamente y llevarla a la posibilidad de incluir dentro de los agravantes de la estafa por medios tecnológicos al artículo 247 del Código Penal Colombiano.

Y así de esta manera poder estudiar este nuevo actuar delincuencial del ciberdelito de manera intensiva y cada uno de los elementos que la componen en el momento de la comisión del actuar delincuencial, utilizando fuentes de información primarias las que se basan en normas jurídicas Colombianas que contemplan el tema del ciberdelito en la estafa y a si mismo jurisprudencia internacional para tener un mejor panorama de la aplicabilidad del agravante en el artículo 247 del Código Penal Colombiano. Como desarrollo de este trabajo de investigación se debe considerar la posibilidad de poder presentar ante el Congreso de la República un proyecto que permita modificar el artículo 247 del Código Penal para poder aplicar dentro de los agravantes de la estafa realizada por medios tecnológicos, un agravante directo y que no continúe en el limbo jurídico al momento de su aplicación, como tampoco tenga que ser adoptado por otras leyes, decretos y normas para poder ser demostradas en un juicio como sucede en la actualidad en el momento de las audiencia preliminares y de preparatoria para un juicio que deben apoyarse en leyes como lo es la Ley 1237 del 2009.

Dicho esto, es pertinente indicar que este trabajo empieza con la demostración del nuevo problema en Colombia y a nivel mundial como son los Ciberdelitos, y como han impactado a la sociedad en especial en la nuestra, ya que hasta ahora estamos empezando a entrar en esta nueva era, por lo que se hace necesario poder iniciar investigaciones y recolectar información a nivel mundial en países que también hayan sufrido este flagelo, y en lo posible que hayan encontrado fórmulas jurídicas con las que hayan hecho frente a este nuevo enemigo que encontramos en la internet.

Lo anterior, se hace necesario para poder adquirir la mayor cantidad de conocimientos que nos ayuden a realizar cambios en nuestra legislación. Podemos decir que este trabajo de investigación puede servir de fuente de información para que los entes gubernamentales encargados de crear nuevas leyes en Colombia, puedan modificar nuestro sistema penal acusatorio, creando la necesidad de la inclusión de este agravante dentro del artículo 247 del Código Penal, ya que es procedente y útil para que la ley sea más directa en el momento de ser aplicada, y no queden vacíos jurídicos que lleguen a generar duda en el momento de su aplicación por los jueces al momento de tener que impartir justicia.

Nuestra sociedad ha empezado hacer uso de estos nuevos métodos de vida como lo es la utilización de medios electrónicos para poder volver a tener una vida comercial normal la cual fue modificada en gran parte a la emergencia de salubridad debido a la pandemia generada por el Covid-19. En este punto, es necesario indicar que este tipo de herramientas es de vital importancia para que la sociedad pueda tener plena confianza para que al momento de realizar transacciones comerciales en las grandes superficies.

Las personas que han sido víctimas de estos ciberdelitos, no encuentran en el Código Penal las suficientes bases sólidas que los lleven a pensar que, al momento de interponer una denuncia

penal por haber sido víctimas de este delito de estafa por medios tecnológicos, tengan claridad sobre los procedimientos tecnológicos y judiciales que adelantan las autoridades para esclarecer este tipo de delitos informáticos.

Frente a este delito de estafa por medios tecnológicos se hace necesario realizar cambios de fondo en nuestras leyes para así de esta manera poder realizar investigaciones encaminadas a buscar todos los vacíos que tiene nuestro Código Penal Colombiano y así de esta manera buscar judicialización de los sujetos activos de estos delitos de manera más efectiva, ya que en la actualidad no existe condiciones directas en la aplicación de los agravantes de este tipo de estafa, siendo el deseo a través de esta investigación, que sirva de sustento en la necesidad de modificar el Código Penal Colombiano en su artículo 247.

Objetivos

Objetivo General:

Establecer el marco normativo y doctrinal en referencia al delito de estafa establecido en el artículo 247 del Código Penal Colombiano y su consecuente agravante cuando para su realización se utilicen medios electrónicos.

Objetivos Específicos:

1. Identificar, la importancia de sancionar de manera directa y a través de la consolidación del agravante por la utilización de medios electrónicos (ciberdelito) en el delito de estafa. Análisis de derecho comparado teniendo como referente España.

2. Estudiar, desde la teoría del delito, el delito de estafa, en la construcción de los lineamientos necesarios para la incorporación del agravante por la realización de este a través de medios electrónicos, de acuerdo con el ordenamiento jurídico Nacional.

3. Determinar la estructura y necesidad de modificar el Código Penal Colombiano en su artículo 247, con la incorporación de un agravante por la utilización de medios electrónicos.

CAPÍTULO I: Reseña histórica del delito de estafa a través de medios electrónicos. Un acercamiento a los ciberdelitos.

1.1. La ciberestafa, una nueva modalidad delictiva.

Para poder entender de manera clara y explícita cual es el contenido directo de la ciberestafa, tenemos, necesariamente que iniciar hablando de su origen y la evolución de estos en un contexto global, para luego, descender y tratar de establecer, de ser posible, quien o cuando se cometió la primera Ciberestafa y desde allí estudiar su evolución. Por ello, se hace indispensable, a efectos de entrar en sintonía, conocer a fondo los orígenes de esta nueva forma de criminalidad, de los que, por supuesto se desprende la referente a la estafa, razón de más, para ahondar en una serie de eventos que han sucedido a través del tiempo, que fueron dando un avance en el perfeccionamiento de estas nuevas maneras del actuar delictivo. Para ello, iniciaremos mencionando el primer registro o acontecimiento de esta clase de delitos en la historia y su evolución en el tiempo. El ciberdelito en la historia de la humanidad no es fácil de plantear o rastrear ya que estos sucesos pudieron haberse generado desde el primer momento en que se creó la internet.

La primera actividad registrada de internet y su creación se remonta al año de 1962 durante la guerra fría y fue descrita en su momento como la “red galáctica” ya que buscaba que todas las personas a nivel mundial obtuviesen información en tiempo real mediante un conjunto de redes interconectadas a nivel global desde cualquier sitio, siendo el primer acercamiento al modelo de internet que conocemos en la actualidad, dando origen a nuestro primer sistema de comunicación por medio de sistemas llamado ARPANET (Red de agencias de Proyectos de Investigación Avanzada). Este, se constituyó en un breve registro histórico de cómo nace la internet a manera de introducción en la exploración y profundización en la investigación de los delitos informáticos a

nivel mundial y su uso en particular, el cual estaba destinado, en un inicio, en compartir información a nivel mundial.

Los comportamientos delincuenciales, sucesos y situaciones cotidianas que se presentan más a menudo en las redes tecnológicas son conocidas como Ciberdelitos, los cuales se llevan a cabo para concretar acciones como hurtos de información personal o empresarial, por supuesto, ocasionados por personas que se especializan en sistemas y utilizan sus conocimientos para ingresar en estas bases de datos y realizar con dicha información obtenida, actos criminales en el espacio digital, mediante redes informáticas y la utilización de diversos dispositivos electrónicos. También, se pueden utilizar para cometer estos actos delictivos programas maliciosos llamados también Malwares que son creados o diseñados con el único objetivo de dañar, borrar o alterar datos sin autorización del propietario de la información.

La primera gran ola de delitos informáticos llego en los años de 1980, cuando se empezaron a crear y organizar grupos de ciberdelincuentes, los cuales vieron este medio para poder cometer sus actos ilícitos, encontrando una gran rentabilidad económica, ya que la realización de dichos actos no les implicaba un gasto económico grande y por el contrario, obtenían ganancias importantes, por lo que vieron en el ciberespacio una gran oportunidad de realizar sus delitos de manera continua y próspera en estos años. Además de lo anterior, se empezó, durante estos años, a implementar el alquiler de equipos de sistemas a diferentes empresas para que pudiesen realizar sus actividades económicas y comerciales de la mejor manera, sin tener que invertir mucho dinero en su uso comercial.

Hacía 1990, los ciberdelincuentes iniciaron sus primeras actividades ilícitas, utilizando a su favor las diferentes necesidades de la época, lo que para los ciberdelincuentes no era nada más

que ver con más facilidad cómo poder realizar sus actividades ilícitas sin que en ese momento las personas tuviesen conciencia de fondo, de cómo era su modus operandi en la web.

1.1.1. Las primeras evidencias en los medios de comunicación.

Pasaron varios años para que se documentaran en los medios de comunicación los primeros casos. Para ello, La revista Welivesecurity (2013), mostró los primeros casos a nivel mundial conocidos de ciberdelincuentes desde el año de 1983 en contra de entidades financieras, haciendo pública la siguiente información:

> En 1995 *Chris Pile* fue condenado en el Reino Unido a 18 meses de cárcel al ser encontrado culpable de crear y distribuir códigos maliciosos. Dentro de los códigos maliciosos se encuentran los virus *Pathogen* y *Queeg* que se cargaban en memoria para afectar los programas que estuvieran en ejecución.
>
> *David L. Smith* fue condenado a 20 meses de prisión en 2002, después de que se declarara culpable de crear y propagar códigos maliciosos. Específicamente fue el creador de *Melissa* uno de los virus que más daño a causado en Internet al afectar miles de cuentas de correo electrónico.
>
> También el año pasado (2012) *Albert González* fue condenado a 240 meses la pena más larga impuesta hasta el momento a un cibercriminal. Albert fue el responsable de uno de los fraudes más grandes de la historia, utilizando técnicas de SQL ingestión logró robar alrededor de 170 millones de números de tarjetas de crédito y claves de cajeros automáticos. (pp. 35-36).

A partir de la publicación de este artículo, se creó la necesidad de indagar más a fondo sobre las crecientes situaciones delictivas que necesitaban ser estudiadas, porque, de ellas se

desprendía que se llevaban a cabo mediante la utilización de medios electrónicos, que por supuesto, escapaban a la reacción de las entidades encargadas de hacerle frente. La respuesta, tal vez, por la falta de conocimiento del asunto, tardó en aparecer y generó como consecuencia la profundización, a través de diversos medios, de publicaciones que permitieron entender la forma en cómo se llevaban a cabo dichas acciones delictivas. A su turno la Oficina de las Naciones Unidas contra la Droga y el Delito UNODC (2013), mencionó:

> Teniendo en cuenta la amplia cobertura de los medios de comunicación, los resultados de varias encuestas que analizaron el alcance y los perjuicios imputables al hurto de identidad, así como los numerosos estudios jurídicos y técnicos publicados en los últimos años, se logró establecer que el hurto de identidad parecía ser un fenómeno del siglo XXI, sin embargo, no fue así. En el decenio de 1980 en la prensa ya se hacía eco del uso indebido de información relacionada con la identidad y de elementos conexos, como el hecho de que en algunos países la falsificación de documentos es un delito tipificado desde hace más de un siglo. Lo que ha cambiado son las estafas a que recurren los delincuentes, el uso cada vez más frecuente de la información digital ha ofrecido nuevas posibilidades de acceso a la información relacionada con la identidad. (p. 13.)

Así como nos lo hace saber la publicación de la revista de las Naciones Unidas, el hurto de la identidad de las personas viene presentándose desde hace varias décadas, en donde siempre, se ha tipificado este delito de la suplantación de identidad como estafa, pero con el transcurrir del tiempo y la implementación y utilización cada día más creciente de equipos electrónicos para realizar transacciones comerciales entre personas naturales y jurídicas, se ha implementado más la estafa, la cual, al ser por medios electrónicos, se le ha denominado en la actualidad como ciberestafa, ya que su medio, en la realización de la conducta es la internet y gracias a ella, las

personas que incurren en esta clase de delitos se han especializado en la suplantación y robo de identidad personal, por lo que la tipificación de este delito se ha vuelto un problema a nivel mundial, con el agravante, de la dificultad que existe para detectar y rastrear a quienes hacen parte de este tipo de organizaciones.

La ciberestafa tiene orígenes nacionales como internacionales, los cuales, se relacionaran con sus diferentes aplicabilidades dentro de este trabajo de investigación, para poner en contexto todo los efectos que tiene este delito en la actualidad y de qué manera se está contrarrestando a nivel mundial, a través de diferentes entidades jurídico penales, en diversos Códigos Penales como el Español y sus continuas actualizaciones, y en nuestro caso, la Ley 1273 de 2009, con la que se creó un nuevo bien jurídico tutelado orientado a la protección de datos y la información. A continuación, se pondrá en contexto toda esta información, iniciando con un artículo de los doctores Ojeda, Rincón y Arias (2010).

> El artículo describe y analiza la evolución del marco conceptual para delitos informáticos propuesto por diferentes autores nacionales e internacionales y establece la relación con la Ley 1273 de 2009 a través de cuya legislación Colombiana coincide con la de otros países en cuanto a que la normatividad contra el ciberdelito como tendencia que afecta no sólo al campo tecnológico sino también al campo económico, político y social. (p. 42)

Es necesario indicar que la estafa es uno de los Ciberdelitos más comunes en la actualidad, y por ello, se debería hacer muchos más énfasis en la forma como ha venido evolucionando el sistema delictivo utilizado para su realización, ya que se ha constituido en unos de los principales sistemas delictivos debido a la creciente ola del uso de las tecnologías en los diferentes aspectos de la vida cotidiana, sin que hasta la fecha en Colombia se hayan creado nuevos mecanismos directos que permitan hacerle frente, los cuales evolucionen al mismo ritmo de la criminalidad. El

resultado, nos dejan sin posibilidades jurídicas al final del proceso judicial de encontrar un autor o un coautor de estos hechos, encontrándonos desde ya, con una problemática muy grave y es que en Colombia no se han tenido en cuenta sus diversas formas para realizar una exhaustiva vigilancia judicial acerca de cuáles son las personas o grupos de personas que utilizan este tipo de espacios para cometer sus actos ilícitos.

En particular, la ciberestafa, realizada esta con medios electrónicos, cuenta en Colombia en la actualidad con muy poca información, ya que su ataque se limitó a la creación de la Ley 1237 del 2009 y hasta ahí, se detuvo la investigación para poder hacerle frente, lo cual es perjudicial para su aplicación ya que la constante modernización en la que nos encontramos, nos deja expuestos a nuevos ciberataques generados desde nuevas redes y plataformas, razón por la cual, se hace necesario que la ley, incluyendo la anterior, no solo se quede en las situaciones antijurídicas pasadas, sino que su aplicabilidad sea cambiante para estar en consonancia a la evolución de estos nuevos conceptos de criminalidad.

Las leyes, deben ser constantemente renovadas para que de esta manera estén a un mismo ritmo frente a delitos que cada día evolucionan, porque aquellas personas que se prestan para su realización no cesan en avanzar con su profesionalización delictiva, por supuesto, que todo ello está encaminado a evitar en la mayor medida posible, ser capturados o descubiertos, por lo que estamos, frente a un auge de nuevos mecanismos delictivos, y sin lugar a dudas la respuesta debe ser contundente, la pregunta en este punto sería, estamos preparados para enfrentarlos, tal vez no, en esta investigación se expondrá el porqué.

1.2. Un acercamiento a experiencias internacionales.

Diversos contextos se desprenden del primer capítulo de esta investigación, sin embargo, según Oxman (2013):

> Lo que interesa destacar aquí es el particular interés que suscitan en la actualidad los fraudes a la banca electrónica cometidos a través de Internet. Se trata de ataques a la integridad y confidencialidad de datos personales, y también, al patrimonio de la entidad bancaria, que afectan la confianza depositada por el titular de la cuenta en la seguridad del sistema financiero para la realización de todo tipo de transacciones. (p. 214)

Teniendo en cuenta que los fraudes o estafas electrónicas están a la vanguardia en todos los países que tengan el más mínimo acceso a internet, debería pensarse en crear una legislación penal acorde con estos delitos electrónicos, los cuales, estén de manera implícita dirigidos a aquellos que se realicen a través de la internet y afecten la integridad y privacidad de todos los datos personales y por el contrario no se tengan que adicionar nuevas leyes ya que de esta manera se es más difícil la actuación del operador judicial.

Por supuesto, que el objetivo principal en esta investigación es la de mostrar la necesidad, de manera urgente, de realizar la adecuación típica de este delito como lo es la estafa informática con sus respectivos agravantes, ya que este modelo de fraude es una de las modalidades del ciberdelito más comunes que ha surgido como una nueva faceta evolutiva surgida de la necesidad de la realización de operaciones por medios electrónicos en el mundo.

La comunicación humana es indispensable y necesaria, ya que vivimos dentro de sociedades evidentemente comerciales, y como elementos de estas, se hace ineludible, aunque existen situaciones restrictivas a la movilidad por situaciones adversas a nuestra voluntad, que el

ser humano no pueda dejar de adquirir productos para su sustento que garantice el mínimo vital, lo cual nos lleva a empezar a realizar transacciones comerciales utilizando medios electrónicos, las plataformas de la internet para toda clase de compras en línea, transacciones bancarias y demás movimientos financieros y económicos, haciéndose necesario que la información personal y financiera se deje expuesta al uso indebido de quienes se dedican a utilizarla indebidamente. La solución no puede estar encaminada a la supresión o limitación de los medios electrónicos, debe, por naturaleza, estar encaminada al entendimiento de estas nuevas formas de criminalidad.

Debido a esto, se hace ineludible crear una urgente necesidad de regulación del manejo de las entidades financieras y de manera general a los establecimientos de comercio, que necesitan de toda nuestra información personal para realizar sus actividades sin que exista la suficiente seguridad por parte de las personas que controlan y regulan el ciberespacio, con plena certeza para los usuarios, qué las transacciones son seguras y pueden ser usadas sin el riesgo de ciberataques.

> Ha surgido una nueva faceta evolutiva de la comunicación, que se halla en una urgente necesidad de regulación, puesto que como el derecho es un producto de la inteligencia y del espíritu humano, no podemos permitir que el ciberespacio haya sido confiado sólo a su autorregulación, puesto que el derecho no permanece inmóvil, sino que se desarrolla y fluye, entonces se debe propender a que vaya variando según las circunstancias de lugar y tiempo, debiendo el legislador hallar las instancias necesarias para hacerlo, puesto que las condiciones cambiantes de la vida, deben llevar a que se reflejen también en el derecho vigente. (Devia, 2017, p. 25).

Dentro de esta etapa evolutiva, se hace necesario y urgente, que se cree una legislación más activa que permita ser aplicada dentro de los delitos que se cometen dentro del ciberespacio y así poder tener un mayor un control sobre todas las actividades de las personas que a este sistema de

internet convergen. La presente investigación se realizó pretendiendo mostrar y nombrar todos los ciberdelitos que de manera antijurídica acompañan el entorno de la ciberestafa como lo son los electrónicos, temáticos, delitos computacionales y los elementos que componen dichos delitos. Cabe resaltar, que el tema que más compete a este trabajo se encuentra relacionado con la imputación objetiva en el delito de estafa informática.

Para Devia (2017), en su análisis a la legislación Española:

> El artículo 248 en su numeral 2 del Código Penal Español, nos permite ver de manera rápida y objetiva la obtención de información básica sobre el fraude cometido por medio de sistemas de cómputo y sobre el tipo penal especifico a la luz de la teoría del delito. La estafa informática, consiste en realizar transferencias no consentidas de activos patrimoniales ajenos, mediante manipulaciones informáticas, materializando así el delito informático y obteniendo beneficios patrimoniales perjudicando a terceros. (p. 26).

Puede tenerse de referencia la legislación penal Española, en donde se observa de manera directa que catalogan a la estafa hecha mediante delito informático como un delito agravado por la actuación directa del participante en dicha acción, que tiene como único objeto la manipulación y aprovechamiento de la información de las personas para hacerlas incurrir en error y obtener de ellos un patrimonio económico indebido. Lo cual sería, el objeto directo del agravante dentro de la estafa. Ahora bien, dentro de las diversas formas de enfrentar este flagelo, se deben entender también diferentes formas de fraude de información, uno de los casos más sonados actualmente es el denominado phishing el cual, según García (2018),

> Se revela como una modalidad de estafa informática cuyo objeto principal es obtener del usuario, entre otros, datos, claves o números de cuentas bancarias con la finalidad de

> obtener un beneficio económico ilícito utilizando para ello de forma fraudulenta y mediando engaño datos personales del usuario. (p. 2).

García (2018) reconoce que “dicha modalidad delictiva ha ido evolucionando con el paso del tiempo, adoptando diferentes perfiles, el cual tiene como objetivo los clientes de Banco y servicios de pago en línea”. (p. 2)

El delito de estafa informática ha surgido a través de diversos mecanismos de realización, los cuales, debido a su constante evolución, se han ido adaptando, constituyéndose en nuevos elementos disuasivos mucho más complejos y modernos, creando de esta manera una mayor dificultad para detectar e identificar cuáles son las personas que realizan la sustracción ilegal de datos personales, lo que hace necesario que se creen nuevos y mejores mecanismos cada vez más sofisticados a la vanguardia de este delito informático, para así poder ser implementados en entidades bancarias y en general, en cualquier tipo de comercio electrónico que permitan la evitación de la sustracción de información que permitan transferencias indebidas no consentidas, donde además, no solo las autoridades a las cuales les compete la creación de esta nueva ciberseguridad, sean también las entidades financieras las que aporten y adquieran nuevos equipos que proporcionen más seguridad a sus usuarios, siendo el phishing la modalidad más utilizada por los ciberpiratas para actuar en este campo.

Actualmente, debido a la necesidad de innovar en sistemas de comercio electrónico que buscan de manera acelerada brindar un servicio más personalizado y menos restrictivo, a la simplificación de procedimientos a través de plataformas electrónicas, han permitido, que el delito económico online sea una de las formas más comunes que utilizan los ciberdelincuentes para poder adquirir dinero de los usuarios que la utilizan debido, por supuesto, a la falta de controles y a la escaza implementación de mecanismos judiciales que permitan hacerle frente.

Los fraudes y las estafas que se llevan a cabo en el ciberespacio, en muchas de las ocasiones, también son realizadas por el descuido de personas y empresas que dejan al descubierto información, el ingreso a sitios de la web que no son confiables o reconocidos, son el foco de propagación propicio, para que, sin realizar la más mínima inspección, se presenten casos de fraude. Es necesario y por supuesto muy importante, invitar a todos los usuarios a verificar de manera certera que el sitio que se va a utilizar proviene de un servidor que brinde las condiciones de seguridad necesarias para realizar el procedimiento requerido. No se trata solo de exigir la intervención de las entidades del estado en proteger, es un hecho que la protección de los datos es un tema que nos debe involucrar a todos de manera mucho más activa, seguro, de esta manera, se pueden evitar actos como los aquí analizados.

Si colocásemos en práctica estas pequeñas, pero muy importantes bases de seguridad y autoprotección personal y empresarial, se pondrían muchas más trabas en la permisión o posibilidad de condiciones idóneas para la comisión de delitos por estos medios y por supuesto, es muy probable, que se evitasen un sin número de acciones criminales que persiguen los dividendos de los usuarios.

1.2.1. La internet. Una peligrosa necesidad.

La internet tiene unas características especiales, las cuales pueden ayudar a que se cometan esta serie de ciberestafas, la primera, según Casado (2017):

> Se refiere a que las características propias que tiene Internet pueden fomentar la comisión de actos ilícitos, la víctima juega un papel muy importante en el ciberdelito, ya que es ella misma la que tiene que llevar a cabo ciertas conductas de autoprotección o medidas de seguridad para reducir las probabilidades de convertirse en el sujeto pasivo de un acto

> ilícito en Internet, más particularmente, puede producirse el hecho de que ésta pierda grandes cantidades de dinero si no plasma de una forma juiciosa sus datos bancarios en el ciberespacio. (p. 3)

La Internet ha cambiado todo en nuestras vidas y en el mundo entero, ya que se ha convertido en una herramienta importante y necesaria para la humanidad en la realización de nuestras actividades personales y laborales de manera directa, al punto, en el que ya son los equipos electrónicos los que influyen en nosotros mismos y en las decisiones de nuestras vidas, sin embargo, hay que tener en cuenta, que es inevitable su utilización, para Evans (2011),

> El impacto que ha tenido la internet en la actualidad en campos como la educación, la comunicación, las empresas, la ciencia, el Gobierno y la humanidad, claramente Internet es una de las creaciones más importantes y poderosas de toda la historia de la humanidad. (p. 2)

Y es debido a la gran necesidad que se ha creado respecto a la utilización de los medios electrónicos para la realización de diversas actividades que han relegado a tradicionales formas de comercio, que se han incrementado las formas en que los delincuentes actúan. Prueba de ello, son las diversas modalidades que se han expuestos hasta aquí, en las que el común denominador, desde la óptica de la estafa, la catalogan como,

> Un elemento clave y diferenciador en el fraude informático, y es que, la transmisión patrimonial no la lleva a cabo la víctima siendo engañada, si no que el propio sujeto activo quien a través de artificios tecnológicos y medios informáticos consigue llevar a cabo tal acción, sin que pueda llegar a existir una fase previa de engaño como sí sucede en la estafa convencional. En estos supuestos que no cumplen los requisitos de la estafa común, el

> engaño y error no están presentes o si lo están es de un modo indirecto, no hay una persona que sufra el engaño ni artimañas encaminadas hacerle incurrir en el error. (Evans, 2011, p. 2)

El mantener en el error, se traduce en la intención de que éste perdure en el convencimiento, idea o razonamiento falsos, en una indebida ideación de que lo realmente sucede a su alrededor, por ende, la acción del sujeto activo se ve encaminada a la intención de la permanencia del error en la acción criminal, se trata de una operación activa dentro del actuar que se dirige a la específica finalidad de que la víctima no salga de su engaño, claro, entre más se vea involucrado en éste, más alta es la probabilidad que perdure la acción y por ende el perjuicio.

> El delito informático ha sido objeto de análisis y por parte de juristas y expertos en seguridad informática, en base a estos estudios muchas legislaciones del mundo han tipificado varias conductas como cibercrímenes. Sin embargo, no existe una clasificación única del delito informático, lo que ha generado que cada legislación le otorgue un tratamiento diferente, no sólo en cuanto a la sanción, si no a la forma de consideración de cada uno de ellos: tanto en las circunstancias de cómo es cometido, como en la forma de investigarlo y procesarlo. Lo dicho lleva a la necesidad de crear una clasificación que intente extraer lo mejor del estudio efectuado por los expertos y lo que el legislador ha tipificado en la normativa penal internacional, abarcando la mayor cantidad de hechos delictuales que pueden ser cometidos con empleo de herramientas informática. (Narváez, 2015, p. 1).

Pero, además de las herramientas introducidas por sistemas extranjeros en la necesidad de crear mecanismos de lucha contra esta nueva forma de criminalidad, debemos reconocer que algunos organismos han entendido que no se trata de una lucha autónoma, que por el contrario

requiere, no solo de la conciencia personal del usuario, sino que además requiere de la participación activa y debida articulación de diversos actores para la estandarización de sistemas de prevención que reconozcan como posible que este tipo de actividades puede surgir de cualquier parte del mundo y en ese sentido deja de ser un delito interno para convertirse en un flagelo global.

Narváez (2015) estudia y reconoce que la "Convención de Cibercriminalidad" realizada en la ciudad de Budapest en el 2001,

> Es el único acuerdo interestatal que aborda la mayor cantidad de áreas sobre ciberdelincuencia, entre la que se cuenta acceso ilícito, interceptación ilícita, atentados contra la integridad de los datos, atentados contra la integridad del sistema, abuso de equipos e instrumentos técnicos, falsedad informática, estafa informática, infracciones relativas a la pornografía infantil, infracciones vinculadas a los atentados a la propiedad intelectual y a los derechos. Sin embargo, en la mayoría no se aborda con amplitud todas las circunstancias como pueden ser ejecutadas. (p. 165)

El análisis, desde la óptica del derecho Penal Español, nos permite llegar a la conclusión que las conductas reconocidas como phishing y pharming se enmarcan en el delito previsto en el Artículo 248.2 del Código Penal Español, en:

> Donde se tipifica la estafa informática. En lo que se refiere al phishing, si bien la mayoría de la jurisprudencia lo ha calificado como tal, un sector de la doctrina estima que en estos casos se trata de una estafa clásica, que se produce al engañar al titular de la cuenta defraudada mediante el envío del mensaje. (Rico, 2012, p. 209)

No por nada, cada día surgen nuevos estudios que nos muestran el impacto que este tipo de delitos están generando en el comercio virtual, miles y miles de personas en el mundo sufren

las consecuencias de los ciberdelincuentes. La problemática, no solo radica en el descubrimiento de diversas formas delictivas, sino en el establecimiento de mecanismos idóneos que permitan la identificación de los responsables. Reconociendo este gran entramado delictivo, Suxo (2009), indica que:

> Cada vez se está haciendo más difícil memorizar los nombres de los nuevos fraudes cibernéticos, y es difícil detectar con algún antivirus o programa. través de este artículo le explicamos nueva técnica de fraude que es el pharming que hace al usuario de Internet más vulnerable, ya que resulta muy difícil identificar cuando uno está en la Red e ingresa a los sitios de su atacante. El fraude consiste en modificar el sistema de resolución de nombres de dominio, con lo que cada vez que introducimos una URL en nuestro ordenador para intentar acceder a una determinada página web, tienda on-line o un banco puede que estemos siendo víctimas de este fraude sin siquiera tratar de darnos cuenta. (p. 1)

A pesar de estas nuevas exigencias en la identificación y necesaria adecuación de nombres que permitan individualizar todas las conductas surgidas de los medios electrónicos como vehículos en la realización de conductas delictivas, es necesario tratar de identificar algunas que nos permitan entender lo difícil de este entramado, pero que nos debe ayudar en la construcción, precisamente de mecanismos preventivos, en el entendido, que al ser identificados, podemos entender cómo hacerle frente y por supuesto, adecuar la legislación en el mismo sentido para, de manera efectiva, hacerle frente.

> El phishing sigue evolucionando y está cada vez más presente en los mensajes que recibimos y también cada vez en un mayor número de países e idiomas. Ahora, su evolución final ha culminado con la aparición del pharming, aún más peligrosa y, en caso de llegar a realizarse, mucho más efectiva que el phishing tradicional, es humanamente

> imposible que se elabore una solución adecuada y a tiempo para algunos códigos que se propagan en cuestión de minutos. La solución para este tipo de amenazas. (Suxo, 2009, p. 3)

Es decir, el reto, se encuentra encaminado a la construcción, como se dijo anteriormente, de nuevos mecanismos preventivos. Sin embargo, uno de los puntos negativos en esta lucha, es que se ha tornado imposible adecuar las normas a la misma velocidad en que surgen estas actividades delictivas, se requiere, por ende, de crear de manera constante sistemas mediante los cuales se detecten las acciones que se llevan a cabo dentro de cada ordenador.

En atención a estas nuevas realidades y entendiendo los nuevos mecanismos de la delincuencia, de acuerdo con Carrillo, Bastidas & Riascos (2019):

> El Phishing, es una modalidad delictiva que genera una gran amenaza para los usuarios de la internet y especialmente afecta el patrimonio económico de las víctimas, es preciso que la Policía Nacional asuma los retos que implica hacer frente a un fenómeno del que poco sabe la ciudadanía y que, de otra parte, está mutando constantemente por la misma evolución de los medios tecnológicos y en esto la institución juega un papel preponderante en el diseño de estrategias que conlleven a cerrar cada día más los espacios a los ciberdelincuentes que se dedican a la comisión de esta modalidad delictiva. (p. 7)

Todos estos antecedentes, nos llevan no solo a pensar en la necesidad de formular reformas en el Código Penal Colombiano, sino a generar mecanismos adicionales, por ejemplo, orientadas a diseñar reformas en la Ley 527 de 1999, (la cual rige en lo relacionado al comercio electrónico, normas electrónicas y mensajes de datos), en lo referente a la tipificación de los delitos electrónicos a fin de que, por el principio de seguridad jurídica, el principio de legalidad, no queden en la

impunidad. Esta es una necesidad urgente y abordar, de manera articulada, las leyes comerciales para que los delitos informáticos tengan un mejor impacto en cuanto a la sanción que pueda impartirse, por tanto, en Colombia, también se deben estudiar las posibilidades de un cambio en las leyes.

La reforma penal a este delito de estafa realizada por medios electrónicos es de extrema urgencia, su modificación en nuestro artículo 247 del Código Penal, sería de suma importancia, y por supuesto, es evidente extender su rango de aplicación en el sistema comercial, para, de esta manera, regular las operaciones que se realicen mediante plataformas o superficies en línea, con una mayor garantía y control al momento en el que se realicen pagos o retiro de dineros. En muchas ocasiones en las que se presentan ciberdelitos, son muy pocas las exigencias que utiliza la página web consultada para autorizar una compra o manejo de dinero por este medio.

Ahora, la necesidad de todo entramado de modificaciones surge de la evidente articulación legislativa que existe en Colombia, muestra de ello, es que la falta de atención en normas que regulan otras materias y que no han sido ajustadas al entorno actual. Ejemplo de ello, es el Decreto 410 de 1971, que establece el Código de Comercio, el cual no ha sido modificado en el entendido de incluir mejoras en cuanto a la seguridad en las transacciones comerciales realizadas en línea, esto protegería mejor a todas las personas que utilizan la internet para realizar todo tipo de transacciones comerciales.

1.3. El phishing, un elemento integrante de la ciberestafa.

Ahora bien, dentro de la diversidad de ciberdelitos, los cuales han sido mencionados de manera general sin entrar en su descripción a fondo, encontramos al phishing, el cual, de acuerdo con Condori (2013),

> Es denominado como un tipo de delito dentro del ámbito de las estafas cibernéticas, y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta, con el objetivo de conseguir de un usuario sus datos, claves, cuentas bancadas, números de tarjeta de crédito, identidades, etc. (p. 34)

Este primer paso, es decir, el buscado para la consecución de la información es la antesala a lo que con posterioridad se conocerá como la estafa. Por supuesto, debe primero accederse a los datos necesarios para culminar con éxito el perjuicio económico que normalmente se persigue con este tipo de acciones. Con posterioridad, a este escalón y atendiendo lo mencionado por la Gerencia de Innovación y Desarrollo Tecnológico (GIDT, 2013):

> El estafador, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantáneo incluso utilizando también llamadas telefónicas (p. 1).

La mejor manera de enfrentar este fenómeno es tomar en cuenta cual es la forma más adecuada de utilizar y seleccionar los proveedores de servicios financieros y cuales son o pueden ser, las entidades comerciales más susceptibles de recibir este tipo de ataques, es decir, mantenerse bien informado en cuanto, cuáles son las nuevas tendencias de ciberseguridad y cuáles son los tipos de ataques de phishing más frecuentes al momento de realizar algún tipo de actividad comercial, que nos pueda contribuir para prevenir las estafas.

Las diversas técnicas utilizadas por los ciberdelincuentes, que les permiten obtener diversa información de los incautos son innumerables, como son innumerables las crecientes formas diversas a la vista, cada día los ciberdelincuentes se encargan de desarrollar nuevas técnicas, las

cuales combinan algunas técnicas clásicas para poder desarrollar diferentes tipos de ataques informáticos, técnicas que competen a esta investigación como son, la Ingeniería social y el Phishing. Para abordar este tema, se hace necesario en este punto, traer a colación el concepto de Giraldo & Duarte (2018), quien considera que:

> Ambas técnicas son vitales para llevar a cabo diferentes delitos informáticos, del cual podemos partir de la base que existe un mundo virtual similar al mundo real, pero en este no existen controles adecuados, ni normas, para controlar dichos ataques razón por la cual somos nosotros quienes decidimos hasta donde y como protegernos de dichos ciber ataques. (p. 10).

En la misma orientación, y profundizando un poco más sobre el asunto, debemos reconocer el progreso y evolución que de estos conceptos se tiene a la fecha, pero que, a pesar de contar con un amplio reconocimiento en esta materia, la discusión se centra en el retraso del establecimiento de mecanismos preventivos. Por ello, para Rico (2012):

> Los avances de la informática y las telecomunicaciones e internet han favorecido el surgimiento de distintas conductas fraudulentas relacionadas con la utilización de medios electrónicos de pago, de encuadrar los nuevos supuestos en los tipos penales tradicionales han motivado la revisión de la legislación con la finalidad de evitar la impunidad de estas conductas delictivas tal como ha ocurrido en la reforma del código penal español de 2010. (p. 1)

Es decir, el fraude informático como lo es la estafa realizada a través de medios informáticos, consiste en la transmisión no consentida de activos, surgida ésta de la indebida manipulación de datos informáticos, lo que se traduce en una conducta paralela a la estafa, en la que la gestión del sujeto activo, de acuerdo con Rico (2012), “guiado por el ánimo de lucro, se

dirige a la provocación de una disposición patrimonial, pero en la que el mecanismo defraudatorio no es propiamente una provocación, mediante engaño, de un error en la víctima, sino la manipulación de un sistema informático". (p. 2)

El surgimiento de estos nuevos mecanismos impone a los usuarios y en general al sistema de control cibernético, el reto de no solo identificarlas, sino de informar y crear las estructuras adecuadas que permitan a los estados hacerles frente. No se trata de una situación pasajera, se trata de una actividad creciente que pareciera no tener fin, si tenemos en cuenta que la internet se consolida cada día más como un elemento de uso cotidiano, traducido este más que como un lujo, como una necesidad, un derecho, con el cual todos, absolutamente todos, tenemos algún tipo de contacto.

El reto, de acuerdo con las condiciones expuestas es la creación de una nueva barrera que nos permita entender y comprender de la mejor manera la forma en cómo funciona el delito y desde allí consolidar mecanismos de protección de los usuarios de las redes. Por supuesto, que, desde la perspectiva del presente trabajo, uno de esos mecanismos está en la intención de emprender nuevos retos legislativos, que nos lleven al fortalecimiento de nuestro Código Penal, y por supuesto, a reconocer como necesaria la modificación en cuanto al agravante del delito de estafa cometido a través de medios informáticos.

Evidente es, que los precedentes nos sirven de reflejo en cuanto a generación de nuevas estructuras legales, no obstante, Colombia y sus especiales condiciones delictivas nos deben llevar a generar las mejores herramientas preventivas y sancionatorias, en este nuevo mundo de la criminalidad, que incluso, sirva de referencia en esta lucha transnacional, que día a día aporta nuevas y mayores retos.

Conclusiones Capítulo I

- La utilización constante de la internet desde décadas atrás ha hecho que todas las personas naturales como jurídicas hayan creado la necesidad de ver a la internet como un elemento esencial en sus vidas diarias tanto personales como laborales ya que es una sistema novedoso y útil lo cual ha hecho que los ciberdelincuentes aprovechen esta oportunidad para realizar toda clase de conductas delictivas relacionadas a los ciberdelitos, los cuales, han visto en las diferentes autoridades que legislan en Colombia, la poca actualización y profesionalización de sus servidores para contrarrestar este fenómeno de la ciberestafa, creando un campo perfecto para que los delincuentes se puedan mover libremente, ya que no existe tecnología actual que pueda frenar de manera directa este delito en particular.

- La tecnología avanza a pasos agigantados buscando siempre modernizar cada uno de sus elementos, cosa contraía, sucede con nuestro sistema judicial y penal ya que siempre se mantiene con las mismas características y no es de un constante cambio, para, de esta manera, estar a la vanguardia de los delitos que con el tiempo si se han transformado y modernizado. Los delitos informáticos se han vuelto un delito constante dentro de nuestra sociedad, sin que a la fecha no se tenga en Colombia ni en el mundo una solución directa para este flagelo.

- La consolidación de nuevas formas delictivas va en aumento, y parece no tener fin, cada día son más nuevos y modernos los sistemas que se pueden utilizar de manera libre y sin ninguna clase de control y son estos los que al estar en manos de personas inescrupulosas y conocedores del manejo íntegro y profesional de estos sistemas les permite cometer toda clase de delitos.

- Referente al marco legal sobre el uso indiscriminado de la internet y de todas la paginas web, ha hecho que los daños económicos realizados por los ciberdelincuentes no se encuentren

regulados dentro de marcos legales y constitucionales, en los cuales, existen meras expectativas de lucha contra estas nuevas formas delictivas.

CAPÍTULO II. Elementos estructurantes del delito de estafa en Colombia.

2.1. Un necesario contexto Nacional.

Para iniciar esta parte de la investigación, Cano Cuervo en el año 2014 en su trabajo de investigación denominado "Aporte internacional frente a los delitos informáticos en Colombia y su ejecución por parte de las autoridades competentes", menciona la necesidad de que las autoridades Colombianas tomen de referencia todas las leyes y normas internacionales para de esta manera nuestra jurisprudencia tenga mucho más soporte legal y jurídico al momento de tener que llegar a la toma de una decisión jurídica emitida por nuestros jueces naturales.

Beltrán & Carrillo, 2017, en su trabajo sobre el acceso abusivo a sistemas informáticos, realizan un excelente análisis de la realidad Nacional, en cuanto a la modificación de las leyes en orientación a las necesidades actuales sociales relacionadas con el tráfico de información en los canales electrónicos, por ello, empleando sus palabras:

> La regulación en Colombia de los delitos informáticos ha demostrado la actualidad de las leyes en este país, pero no se ha permitido avanzar mucho en la tecnología que se necesita realizar una correcta y veras investigación en contra de estos delitos que requieren de tiempo, capacitación y conocimiento especial de programas irregulares o ilegales. (p. 6)

Realmente, Colombia debe tener en cuenta los aportes de las diferentes investigaciones judiciales que se realizan frente a este delito de la estafa informática, para que de esta manera se cree la necesidad jurídica de la modificación a los agravantes de esta conducta atípica.

En Colombia, existen yerros jurídicos que van en contravía a la debida aplicación de la jurisprudencia en cuanto a esta clase de nuevos delitos que nos trae la globalización, en donde nos damos cuenta de que el ciberespacio es un lugar el cual Colombia no ha podido utilizar en beneficio

propio, para así poder estructurar mecanismos de protección frente a este tipo de flagelos. Siendo esto así, son evidentes los vacíos jurídicos que facilitan que algunos actores infrinjan la ley en estas circunstancias y por supuesto puedan eludir el alcance de la justicia.

Para González (2014), "Colombia se encuentra entre los 5 países latinoamericanos con mayor número de incidentes de seguridad tales como: fraude electrónico, extorción, robo de información, denegación de servicio, malware, virus entre otros" (p. 1). Lo que supone, que nuestro país no está en un constante cambio de las leyes existentes para estar a la vanguardia de los nuevos delitos, que permitan contrarrestar la gran cantidad de Ciberdelitos que se presentan en la actualidad y claro, no se ha dado la suficiente importancia que permitan ser investigados de manera más verás y efectiva, en el entendido que la nueva generación de usuarios de la internet es mucho más elevada, incrementando las posibilidades de actuar de los ciberdelincuentes.

Los nuevos ciberdelincuentes se están capacitando cada día de la mejor manera para cometer estos delitos, orientados en la estructuración de mecanismos que les permitan dejar la menor cantidad de rastros en la web, lo que, sin dudas, los hace mucho más profesionales en este sentido, sin que hasta el momento se les dé la suficiente importancia, siendo delitos vanguardistas de nueva generación, que ven en está forma de delinquir un vacío jurídico dentro de la legislación penal Colombiana.

La realidad por la que atraviesa el Estado Colombiano muestra, de acuerdo con González (2012),

> Un panorama devastador, encontramos que el gobierno presenta debilidades informáticas y cibernéticas, no se observa que se están creando mecanismos para contrarrestar este tipo

> de debilidades, que se trabaja constantemente en el desarrollo de nuevas prácticas para fortalecer la seguridad de la información. (p. 3)

Los mecanismos que está utilizando el gobierno para mejorar este ciber problema, es el de empezar a mejorar todas las falencias que tiene la legislación Colombiana para, de esta manera, perfeccionar la seguridad informática y la seguridad de datos personales y crear elementos que puedan contrarrestar de manera efectiva los intentos de fraude.

Una de las prácticas actuales de seguridad frente a estos delitos, tanto de las personas jurídicas como naturales, es la no facilitación de información a ninguna fuente desconocida, ya que esta sería la mejor forma de auto protegernos frente al ciberdelito y la estafa informática.

Este delito, comprende todos los actos delictivos que se realizan para poder cometer el ilícito y así de esa manera poder obtener dinero de manera fraudulenta, lamentablemente, en Colombia, en contraste con la legislación Española, en materia penal no se cuenta con leyes que permitan robustecer los artículos ya existentes como es el caso del 247 del Código Penal, en el que se reconocen los agravantes de la estafa, sin que en dicho artículo se encuentre tipificado el cometido utilizando medios electrónicos.

Tampoco, dentro de los agravantes de la estafa en nuestro Código Penal Colombiano, se encuentra suscrito el delito de estafa por suplantación de sim card, el cual consiste en hacerse pasar por el titular de la cuenta y se acercan a la empresa de telecomunicaciones para que esta les proporcione una nueva sim card y de esta manera puedan adquirir productos y servicios de las empresas de telecomunicaciones como por ejemplo, obtener teléfonos celulares de alta gama para luego ser vendidos y llevar a cabo la estafa. Estos son ejemplos de la manera en cómo ha avanzado la criminalidad a través de medios electrónicos, es indudable que nos encontramos en un mundo

que ve cada día un sin número de oportunidades para los delincuentes y nosotros, estamos relegados y a la merced de los avances que en este sentido se presenten.

Para Morales (2020), “según datos de la firma de ciberseguridad Kaspersky, ha habido un aumento del 30% en el número de delitos de ciberestafa en todo el país desde que el Covid 19 se volvió una pandemia” (p. 1) lo que generó un impacto importante en la necesidad de las personas en empezar a utilizar toda clase de medios electrónicos para poder estar informadas y poder realizar toda clase de transacciones comerciales utilizando las plataformas tecnológicas que existen en el actualidad, lo cual hace que las estrategias de ingeniería social sean más utilizadas por los delincuentes en la red.

Citando a Barrios (2012), en la investigación realizada acerca de las tendencias de estafa a nivel mundial:

> El tema de la defraudación mediante la utilización de medios informáticos es un tema que mantiene dividida a la doctrina que se ocupó en la materia, ya que para algunos es una situación que encuadra en la Estafa Genérica, sin necesidad de entrar a estudiar reforma alguna, ya que es innecesaria, de modo tal que la estafa informática, es una estafa genérica, que sólo se diferencia de la otra en que el medio utilizado es un medio informático, ya que lo que se tiene en cuenta es el fin. (p. 33)

Es claro entonces, y a efectos de consolidar el contenido estructural de la investigación, que la estafa informática se puede originar desde cualquier parte del mundo, aunque su realización se lleve a cabo de diversas formas, siempre, se hará necesario el uso de la internet para poder lograr el objetivo principal de la ciberestafa, que es el hurto de información y luego, mal utilizarla y

cometer hechos ilícitos que atentan directamente, en la mayoría de los casos, en el patrimonio de los afectados.

Ahora bien, como enfrentar de manera probatoria un adecuado establecimiento de elementos que permitan la demostración del hecho. Dicho en palabras de Sáenz & López (2018), "establecer los desafíos que enfrentan los operadores de la justicia Colombiana, para la obtención de la prueba penal, en materia de delitos informáticos" (p. 26), hace pensar de qué manera, se debe llevar a cabo la debida recolección de la prueba para estos ciber delitos ya que en la legislación de Colombia no existe un formalismo especial como tampoco un manual de cómo se debe realizar una correcta recolección del material probatorio, que robustezca las investigaciones que se adelanten y que tengan la validez suficiente a la hora de ser llevados a un juicio, sirviendo como prueba penal legalmente recolectada, evitando que no se vuelva este procedimiento un desafío para los agentes del estado que realicen la investigación de los Ciberdelitos. Así como también para los señores jueces de la República a la hora de aplicar la ley, si no por el contrario le sea mucho más práctica la dinámica de la prueba en estos actos.

Ahora bien, la Ley 1928 de 2018, aprobada por el Congreso de la República de Colombia y en la cual se señala la adhesión al Convenio de Budapest, constituye la principal herramienta a nivel mundial, con la que cuentan los países que se unieron para combatir los delitos informáticos y todas sus implicaciones, ya que se puede compartir y recopilar información entre los países firmantes para robustecer nuestras leyes y nuestro Código Penal para hacer más efectivo su aplicación.

La vinculación del estado Colombiano al convenio de Budapest, aporta en el avance, junto con otros países que sufren este flagelo, de grandes pasos en la creación de nuevas y más efectivas leyes que coadyuven a localizar y recolectar material probatorio y en el establecimiento de

mecanismos preventivos y de persecución a los ciberdelincuentes en compañía de los países aliados, para la recolección de información apropiada para combatir estaos delitos de la web con más precisión y efectividad y ser aplicado esto en nuestra justicia penal actual.

Respecto de la prueba, y de acuerdo con Rendón (2012) ¿Qué dificultades presenta la prueba digital en el proceso penal en cuanto al decreto, práctica y valoración dentro del sistema procesal Colombiano? La respuesta, surge de la vital importancia en definir este tipo de parámetros, teniendo en cuenta que no se tiene en la jurisprudencia Colombiana mecanismos actuales para llevar o presentar ante un juicio una prueba digital por un delito cibernético cometido por los ciberdelincuentes. Es así como, se sustenta la inclusión del agravante del ciberdelito dentro del delito de estafa, ya que surge como una herramienta útil y necesaria en la práctica y realización de un juicio, en donde se aporte como prueba una digital y generar, de esta manera una decisión más asertiva de los operadores judiciales.

Empleando palabras de Díaz (2010):

> Se dejaron finalmente siete de los diez artículos que originalmente habíamos sugerido, se excluyeron tipos tan importantes como la falsedad informática, espionaje informático y el spam, le modificaron el epígrafe a la estafa informática por transferencia no consentida de activos. Por fortuna no se tocó el que considero uno de los más importantes adelantos legislativos del país, con el derecho penal comparado, la violación de datos personales, pues nos tornamos en uno de los pocos países en el mundo de darle una protección penal a los datos personales, pues otras naciones se la dan administrativamente con las Agencias de Protección de Datos Personales en donde existen, Colombia es huérfana con este ente. (p. 1)

Surge del anterior análisis, que la Ley 1273 de 2009, no cumplió con la eficacia esperada, ya que como lo dice el autor, el artículo no fue puesto en práctica en su totalidad, consolidando el criterio acá expuesto de la necesidad de la actualización de la legislación nacional para que se normalice su uso, ante el cambiante mundo del ciberdelito no solo Colombia sino de manera global.

De acuerdo con Bustos & Torres (2018):

> En la aplicación del derecho penal, es importante tener en cuenta la evolución de los tipos penales y las nuevas formas de cometer fraudes por medios electrónicos, por lo cual la legislación tiene que ser actualizada permanentemente para lograr sancionar a los sujetos que infringen por cualquier medio electrónico ocasionando un daño antijurídico y culpable. (p. 2)

De esta manera, se busca consolidar los aspectos más relevantes en la necesaria estructuración de los pilares que permitan generar la necesidad de modificar el Código Penal en su parte pertinente, y tener un concepto claro sobre cual es y cómo se desarrollan los delitos informáticos, y englobar un concepto con el que se permita determinar cuál es la forma general del concepto de este delito, y hacer un recorrido sobre la evolución legislativa hasta dar con la Ley 1273 de 2009. La evolución de los nuevos delitos informáticos y su realización por medios electrónicos está llamada a mantenerse en una permanente actualización jurídica, para que, de esta manera, los delitos informáticos no ocasionen daños severos, y poder agrandar el cerco jurídico en contra de los ciberdelincuentes.

En cuanto a su estructura, el delito de estafa en Colombia hace parte de aquellos delitos establecidos en el Título VII del Código Penal, en donde el bien jurídico tutelado es el patrimonio

económico. En el Código de 1936, este tipo de infracciones estaban encaminadas a la protección de la propiedad, en las que se reconoce la posesión, la mera tenencia, el usufructo. Etc. De acuerdo con la norma en cita, todo aquello que pertenece en forma directa al individuo, conforma ese haber de especial protección desde la óptica de este título.

El concepto de estafa proviene del Derecho Romano en el que se reconocía como *crimen stellionatus,* en el que se sancionaba el provecho indebido obtenido a través de engaño. Fue solo hasta el año de 1822 en el Código Penal Español, que se implementó por primera vez el nombre de estafa, en el que de igual manera se imponía una sanción para quien afectara de manera grave el patrimonio de un sujeto a efectos de obtener provecho ilícito, por supuesto que la concepción tan elaborada fue construyéndose de manera clara y concreta con el paso del tiempo. Sin embargo, el efecto directo del reconocimiento de la estafa siempre ha estado orientado a la afectación del patrimonio.

En estricto sentido, el patrimonio involucra un conjunto de bienes que por supuesto, dados los avances de la tecnología, han trascendido a aspectos virtuales, en los que se reconocen las transferencias de datos, en el que por supuesto están aquellos que representan valor monetario.

Para Bustamante (1979), al establecer las características de lo que debe reconocerse como ese conjunto de bienes, menciona que:

> Es más exacto decir que el patrimonio es la universalidad jurídica que comprende todos los bienes, objetos exteriores que pertenecen o corresponden a una persona: pecuniarios, intelectuales o morales, sin perjuicio de que tales bienes puedan estar sometidos a tratamientos jurídicos diferentes según su naturaleza o contenido. (p. 31)

Sin embargo y a pesar de que la connotación abierta de lo que conocemos como patrimonio, no implica necesariamente el establecimiento de una medida de aplicación de lo reconocido en el Título VII del Código Penal. Allí, su enunciación registra de manera clara que, para efectos del interés penal, solamente abarca al patrimonio en relación económica, es decir, nos interesa únicamente, aquellos aspectos en los que se toca la economía del sujeto. Para nuestro estudio, es importante mencionar que, dentro de las concepciones importantes para el estudio del derecho penal, existen teorías mixtas jurídico – económicas de patrimonio. De acuerdo con Muñoz (1995), esta línea de pensamiento reconoce aspectos como:

a) Objeto material de un delito patrimonial sólo pueden serlo aquellos bienes dotados de valor económico.

b) Para ser un sujeto pasivo de un delito patrimonial no basta con que el sujeto tenga una relación meramente fáctica con la cosa: es preciso que esté relacionado con ella en virtud de una relación protegida por el ordenamiento jurídico.

c) Por perjuicio patrimonial hay que entender toda disminución, económicamente evaluable, del acervo patrimonial que, jurídicamente, corresponda a una persona. (p. 226)

Ahora bien, para que exista perjuicio, la acción debe consistir en el provecho ilícito que se obtiene, mediante la utilización de engaños, con la suficiente entidad para producir efectos que permitan la consecución del hecho perseguido, es decir, que admita inducir a un sujeto al error. No obstante, y para entender de mejor manera el delito de estafa, se hace necesario estudiar su estructura y los elementos que lo integran.

2.2. El delito de estafa. Estructura típica.

En su clasificación se establece que el tipo es de resultado, es decir, que se requiere que efectivamente se presente lesión en el patrimonio del sujeto pasivo de la acción. Se trata de un tipo mono-ofensivo, en tanto protege, como verbo rector, al patrimonio económico, aunque pudiera entenderse que éste, al proteger tanto la verdad y la buena fe, pudiera catalogarse también como pluriofensivo. Así las cosas, la consumación del hecho delictivo se realiza con la obtención del aprovechamiento ilícito de la acción, sin embargo, de presentarse circunstancias especiales en su no realización se permitirá como posible la tentativa.

La estafa, como tipo penal autónomo, requiere para su configuración, la comprobación de una serie de pasos, conocidos estos como relación causal ideal, los cuales imponen su estricto acatamiento, ya que, de no presentarse de esta manera, es posible que no pueda hablarse de estafa. Estos elementos son, de acuerdo con la sentencia proferida por la Sala de Casación Penal de la Corte Suprema de Justicia (2006), los siguientes:

i) el uso del engaño por parte del sujeto activo;

ii) de ello, se deriva el hecho de mantener o inducir a error al sujeto pasivo, por los artificios o engaños del sujeto activo;

iii) Como consecuencia de lo anterior, el sujeto pasivo debe desprenderse total o parcialmente de su patrimonio voluntariamente;

iv) lo que genera un provecho ilícito económico (resultado material) para el sujeto activo, o un tercero. Finalmente;

v) que dicho desplazamiento patrimonial cause un perjuicio ajeno correlativo.

De lo expuesto, surge como necesario que se estudien unos elementos comunes en la causación del daño, como lo son el engaño, la inducción al error, el perjuicio y la obtención del provecho ilícito como descripción del tipo.

2.2.1. El Engaño.

Hemos entendido, con la simple lectura de la descripción del tipo, que, para la consumación del delito de estafa, debe presentarse un artificio o engaño. Para algunos sectores de la doctrina, ambos términos son sinónimos, sin embargo, el legislador utilizó con total conocimiento la utilización de las dos palabras en la descripción del delito en el Código Penal. El artificio, según la Real Academia de la Lengua, es la habilidosa, astuta y calculada transformación de la verdad. En ese sentido, el sujeto activo de la acción debe desplegar una conducta intencional con la única finalidad de mostrar algo que no es real. Por otro lado, el engaño, está orientado a hacer ver que tal artificio parezca verdadero, de entrada, en las dos concepciones, se observa una conducta dolosa, debido a la intencionalidad y conocimiento del hecho que se pretende ejecutar.

Hay que tener en cuenta que, en el engaño, es importante que se muestre una credibilidad certera que permita mostrar como idóneo el acto con el que se presente consolidar la maniobra fraudulenta, que se produzca de manera constante este o se mantenga en error como un elemento necesario en la demostración de lo que se conoce como estafa. Ahora, ¿qué sucede cuando el sujeto activo no es quien indujo en error a la víctima?, pues, la doctrina y la jurisprudencia han abordado el asunto, asumiendo que el omitir (sacar del error) al sujeto pasivo, también constituye, a manera de omisión, la consolidación del hecho y por supuesto la estructuración del delito.

De acuerdo con los postulados de la imputación objetiva, no cualquier engaño puede ser tenido en cuenta como generador del tipo penal, para ello, se requiere, como se expresó líneas

atrás, que ex ante, la conducta cree un riesgo no permitido o reprochable frente a un bien jurídicamente protegido, por lo que, la maniobra o engaño debe tener la virtualidad de inducir en error al sujeto con la correspondiente afectación en su patrimonio, es decir, la simple mentira no constituye en sí la consumación del tipo. Como lo afirma la sentencia 17196 emitida por la Sala de Casación Penal de la Corte Suprema de Justicia (2003), "Solo cuando la peligrosidad del engaño sobrepasa los deberes de la autoprotección -actuar del hombre medio o profesional-, se está ante un engaño penalmente relevante".

2.2.2. Inducción al error.

Éste, de manera primordial debe ser determinante, no cualquier error puede ser considerado como tal para generar un perjuicio que involucre la acción penal. El error, debe contener para el sujeto activo la connotación de tener nociones o ideas falsas de la realidad, lo que en ocasiones puede llevar a confundir el error con la ignorancia, ya que ésta es el alejamiento total de la realidad, por lo que estos casos, el sujeto pasivo debe poder comprender la condición a la que fue sometido. En términos generales el error debe ser impuesto, es decir, que se haya generado como consecuencia del accionar de un sujeto con la intención de generar un perjuicio y obtener un provecho ilícito.

2.2.3. Perjuicio.

Para el profesor Leyton (2014) "el perjuicio consiste en una disminución del patrimonio del sujeto pasivo, pérdida que debe ser apreciable pecuniariamente, es decir, expresada en un valor económico, quedando descartadas, por ejemplo, las meras expectativas, al no ser comprendidos dentro del elemento del tipo". (p. 153)

El delito de estafa atenta directamente y por expresa disposición contra el bien jurídicamente tutelado del patrimonio económico, por lo que la acción criminal debe recaer sobre éste, en lo que, de acuerdo con la doctrina, debe cobijar a la posesión y a la mera tenencia, por su consecuente valoración en términos económicos. Es importante recordar que el perjuicio debe surgir del engaño, porque a partir de él se empieza a consolidar todo un entramado que debe estar dirigido a la afectación de su patrimonio.

2.2.4. Provecho ilícito.

Según Pabón (2013), de acuerdo con la estrecha relación existente entre perjuicio y provecho:

> El provecho es un término normativo que consta de un elemento fáctico y uno jurídico. Fáctico, ya que el despojo patrimonial debe ser palpable y mensurable derivado del engaño; jurídico, pues la desposesión la debe aprovechar el sujeto activo o un tercero que lo obtuvo a través del engaño, por lo que el hecho resulta ilícito y reprochable en materia penal. (p. 360)

Así las cosas, el provecho es el beneficio que obtiene el sujeto activo y por supuesto, el perjuicio, aquel que sufre el sujeto pasivo, sufrido con ocasión a la puesta en marcha de una serie de acciones, que, de no haberse llevado a cabo, o presentarse la verdad, es decir, sin engaño, no se habrían podido consumar. Es importante siempre resaltar que éste, el provecho, debe ser patrimonial y el objeto de la estafa debe ser ilícito.

2.3. Elementos objetivos del tipo.

Para enunciarlos y a afectos de no generar un cúmulo innecesario de subtítulos, se mencionarán de manera correlacionada en una sola narración, en la que se espera se comprenda de manera efectiva los elementos que integran este importante aspecto.

La conducta contiene un verbo determinador simple, que está enmarcado en la obtención de un provecho ilícito con perjuicio del patrimonio de un sujeto. Esta conducta es de las llamadas de resultado como se indicó letras atrás, por lo que se requiere la efectiva consecución del beneficio económico y por supuesto el detrimento mencionado. Ahora bien, el verbo "obtener" indica la realización de una acción en conseguir un beneficio, perfeccionado con la afectación del patrimonio, por lo que el objeto material del delito es personal. Es la persona inducida en error o mantenida en él quien asume como objeto de la acción. Por supuesto que este delito admite que los sujetos pasivos sean diversos, en los que habrá también que diferenciar, que es posible que suceda, que exista diferencia entre quien se mantiene en error y quien sufre el perjuicio.

Como elemento normativo encontramos que el beneficio obtenido por parte del agente para sí o para un tercero debe ser ilícito, esto reitera el concepto antes mencionado en el entendido de comprobarse algunos elementos necesarios para su demonstración, en lo que se refiere a este delito, se requiere. Aquí lo importante es que el sujeto activo no tenga ningún tipo de soporte de naturaleza jurídica que le permita recibir el beneficio, ya que, de ser así, se desnaturalizaría la estafa. Visto de esta manera, el perfeccionamiento de la acción queda agotado con el aprovechamiento ilícito económico y la afectación del patrimonio.

Hasta este punto hemos hablado de los elementos necesarios para la consumación del hecho, sin embargo, no hemos expuesto circunstancias especiales de quienes se involucran en el

acto. Y es que, es preciso que se mencione, así sea de manera somera, porque no requiere mayor profundidad, tanto al sujeto activo como al pasivo en el delito. Basta con mencionar que el activo, el agente, no contiene en sí cualidades especiales y muy por el contrario puede ser cometido por cualquier persona.

Respecto al sujeto pasivo, es necesario mencionar, de acuerdo con Suárez (2013), que "el titular de la relación posesoria cuyo objeto, derecho de crédito o servicio sea aprovechado ilícitamente por el sujeto activo, quien logra la realización del acto de disposición patrimonial de parte del engañado". (p. 315), por lo que no necesariamente quien sufre el engaño es quien en últimas es reconocido como sujeto pasivo, por lo que se debe mirar al titular del bien jurídicamente tutelado.

La identificación de estos elementos nos permiten diferenciar las diversas facetas que puede presentar la consumación de este delito, la construcción y determinación de ellos, nos llevan, también, a mirar de una manera diferente aquella actuación cometida a través de medios electrónicos, situación que implica un conocimiento de las diferentes opciones con que cuentan los criminales para su realización, pero que concuerdan en la necesidad de la comprobación tanto de la ideación como de la afectación a través de engaño.

2.4. Elementos subjetivos del tipo.

Hemos visto como esta conducta requiere para su realización, la ideación y ejecución de una serie de actividades que demanda tanto del conocimiento como de la voluntad para la consecución de un fin, en este sentido, surge evidente que el elemento subjetivo del tipo es el dolo, porque se lleva a cabo con el pleno convencimiento de la ilicitud de la acción, lo que concuerda con la definición que de dolo hace nuestro Código Penal.

Sin embargo y a pesar de parecer simple el análisis que del elemento subjetivo del tipo se hace, es pertinente abordar este punto de la mejor manera, a efectos de entender a ciencia cierta las diferentes aristas que surgen o pueden surgir a partir de su valoración y entender por qué es tan importante en la determinación de la conducta.

En este orden de ideas, debe abordarse el asunto a efectos de identificar aquellas zonas grises entre el dolo y la imprudencia, ello, como presupuesto necesario en la identificación del responsable de la acción, así como algunos elementos cognitivos y volitivos que no pueden identificarse tan fácilmente. Para ello, conoceremos diversos momentos en la identificación de la ideación del hecho y posterior consumación.

2.4.1. Momento intelectivo.

En él concurren el conocimiento, la representación y visualización del hecho, es decir, el sujeto conoce las consecuencias de la violación de la ley penal y la afectación del bien jurídico. Éste conoce, las características especiales del tipo, "el objeto jurídico, los ingredientes normativos y los complementos subjetivos se han de comprender en su significación conforme a la experiencia común, a las normas culturales imperantes o a su noción jurídica elemental. (Arteaga, 1975, p. 121), es decir, se exige el conocimiento de la antijuridicidad del acto, que evidencia su conocimiento de la violación de la ley.

2.4.2. Momento volitivo.

Consiste en la actitud consciente del sujeto activo de la acción, es decir, que éste pretende la realización del hecho, como mecanismo de obtener para sí o para un tercero un provecho. Todo aquello que le sirva al sujeto para estructurar el tipo, en tanto lesión patrimonial, sin que medie justificante jurídico, tendrá incidencia en el momento volitivo.

> La volición en el dolo es en verdad aquella voluntad incondicionada para la realización del tipo objetivo, en la consciencia de su posibilidad efectiva; cualquier falta de decisión para realizar el hecho o la consciencia de su imposibilidad, excluyen el dolo por falta de volición, la cual se observa también cuando el hecho se presenta materialmente como imposible; nadie puede querer lo desconocido, ni conocer y querer lo irrealizable o inejecutable. (Pabón, 2013, p. 386)

2.4.3. Momento ejecutivo.

Este momento constituye, en la ejecución del acto criminal, el juicio práctico que surge como consecuencia de la manifestación real de la voluntad en querer la realización del hecho. Surge de la proyección de la ideación y la consecuente ejecución del acto que por supuesto luce antijurídica (dolus malus).

Ahora bien, en este punto se hace necesario no solo identificar los aspectos relevantes que se generan hasta la consolidación del acto criminal, sino conocer cómo y de qué manera se presenta la intención, para entender las razones que nos pueden llevar a determinar el verdadero propósito del actor frente a la ejecución de la acción.

2.4.4. El Dolo.

La doctrina ha desarrollado ampliamente los conceptos de dolo en la forma como el sujeto activo de la acción actúa y de qué manera este manifiesta su voluntad en la ejecución o consolidación de la ideación criminal.

Desde esta óptica, se han identificado diversas formas de manifestación de la voluntad que desde el punto de vista de la doctrina y también de la jurisprudencia, nos han permitido establecer diferencias y fenómenos que rompen con la percepción tradicional del dolo. Ello, como muestra

de una serie circunstancias que afectan la intencionalidad del sujeto cuando éste no representa en sí, la misma intencionalidad en la actividad que se despliega con la consecuente afectación del bien jurídicamente tutelado.

Para entender un poco mejor el asunto y a manera de información, teniendo en cuenta que se entiende que la intención en los delitos informáticos en especial en el de la estafa, por supuesto que está ligada a la clara voluntad y conocimiento de la realización del hecho. Sin embargo, este tipo de información se considera importante en el entendido de determinar de manera certera en qué postura se encuentra el agente.

2.4.4.1. Dolo malo y dolo bueno.

Se entiendo por dolo bueno aquella acción en la que el sujeto actúa motivado por razones altruistas y no con un propósito ligado a la violación de la ley con resultados antisociales. Existen conductas reconocidas en el Código Penal que lo reconocen, como es el ejemplo del homicidio por piedad. De otro lado, el dolo malo, se traduce en la intencionalidad negativa en la realización y consecuente perjuicio social.

2.4.4.2. Dolo de ímpetu y dolo de propósito.

En el primero, la voluntad criminal surge de manera súbita, no existe una ideación previa de consolidación de la intención, aquí, en el momento en que surge la consecuencia es la ejecución del acto.

En el dolo de propósito en cambio, existe una ideación simple en la que el actor realiza una deliberación más o menos ponderada de su intención en la consumación de un acto criminal, es decir, el agente ordena y estructura una serie de medios que le sirven en la ejecución a manera de oportunidad para la realización, es, sin duda, la premeditación de la actividad orientada a la

vulneración del bien jurídico tutelado. Para Mesa (1979), de acuerdo con la teoría clásica, la premeditación debe contener:

> La resolución de cometer el delito, el transcurso del tiempo considerable entre la resolución y la ejecución criminosa, el ánimo frío y tranquilo y la reflexión sobre la forma de comisión, los medios que se van a emplear y las circunstancias que aseguren mayor eficacia. (p. 114)

2.4.4.3. Dolo inicial, concomitante y posterior.

El dolo inicial se refleja únicamente en la ejecución inaugural de la acción criminal, en términos generales puede asociarse con el dolo de ímpetu, ya que su manifestación se presenta de firma clara en los delitos de ejecución instantánea. El dolo concomitante, se traduce en el resultado de la acción, ya que los acompaña hasta la culminación del resultado, es decir, hasta su consumación, lo encontramos expresamente expuesto en los delitos de resultado o de ejecución continuada.

Finalmente, el dolo posterior, a pesar de no estar reconocido en la mayoría de la doctrina, es aquel que se manifiesta posteriormente a la acción. La razón, luce simple de acuerdo con algunos expertos en materia penal, para Mesa (1979) “el dolo subsiguiente no existe, él empieza cuando comienza la ejecución de la conducta delictiva”. (p. 115) es importante señalar que sucede algo similar con la clasificación realizada por algunos doctrinantes en lo que se conoce como dolo genérico y dolo específico. El primero se encuentra inmerso en la intención del agente, sin embargo, en el segundo se requiere de la acreditación de ciertas infracciones del sujeto activo con una especial finalidad, por lo que no ha sido aceptado como posible en la medición de la intencionalidad del hecho delictivo.

2.4.4.4. Dolo directo y dolo eventual.

En el directo, el resultado de la conducta criminal concuerda expresamente con la intención del agente. Es decir, en él se conjuran claramente los dos elementos básicos del actuar doloso, conocimiento y voluntad. El actor quiere el resultado y ejecuta una serie de acciones tendientes a su consolidación, con la consecuente afectación a los bienes jurídicamente tutelados, en resumen, es la manifestación directa del actuar criminal con el pleno convencimiento de que su actuar, fuera del contexto legal, representa un hecho delictivo que debe ser castigado.

El dolo indirecto o eventual, fue reconocido inicialmente en el artículo 36 del Código Penal (1980), reconociendo que "la conducta es dolosa…, cuando la acepta previéndola al menos como posible". No obstante, con la modificación incluida en el Código Penal (2000), se modificó un poco la estructura de lo allí consignado y el artículo 22 se plasmó "también será dolosa la conducta cuando la realización de la infracción penal ha sido prevista como probable y su no producción se deja librada al azar".

Aquí, existe una especie de menor intencionalidad en el querer del sujeto activo de la acción respecto del resultado pretendido, ya que el agente mismo no quiere producir el daño consecuente, es decir, existe una aceptación del riesgo. Para muchos, no solo se trata de dejar al azar, porque en esa intención puede estar inmersa una postura de desinterés que debería ser estudiada a profundidad como si se tratara de una omisión en la intención de evitación del daño. Para otros, es una zona en la que se mezclan tanto el dolo como la culpa, y el que la diferenciación de uno y de otra estará representada por la representación de la probabilidad del daño o resultado.

Las apreciaciones hasta aquí expuestas nos sirven de sustento en la diferenciación de algunas concepciones básicas en la presentación de los hechos delictivos descritos en la estafa.

Hemos visto cómo la ideación de la actividad criminal, en lo referente a la estafa a través de medios electrónicos, representa un icono en los actuales mecanismos delictivos, ya que para su consumación se requiere, además de la voluntad, de una serie de conocimientos específicos que le permitan al agente acceder a información privilegiada, a la estructuración de las plataformas necesarias y ello, sin lugar a dudas representa de manera concreta el estar frente a un delito en el que el elemento subjetivo es el dolo en la categoría de directo.

Todos estos complementos ligados al comportamiento humano son los que justifican dogmáticamente su presencia en la subjetividad de la acción, ya que no solo basta demostrar que un comportamiento atenta contra un bien jurídicamente tutelado, sino que se requiere que exponer la finalidad de la acción y cómo se estructuró en la mente del agente para luego llevarla a la consumación. El estudio de las actuaciones penales no solo puede limitarse a la demostración de la violación legal, se debe llegar a la exposición clara y concreta de los hechos que rodearon la actividad y si esta se consumó a través de una ideación expresa y con fines destructivos o si por el contrario surgió como consecuencia de un actuar imprudente, por ejemplo, lo que sin duda y para el estudio del delito de estafa, sacaría por completo del contexto la necesidad de demostrar la intención del estafador en la consumación del acto porque cambiaría la calidad de éste.

Son muchos los conceptos que brindan una claridad sobre el tema y aunque pareciera simple, la demostración del conocimiento y voluntad, para algunos, de acuerdo con manifestaciones mentales diversas, no permite de manera tan sencilla determinar en qué momento el sujeto actúa consciente o inconsciente. Estos conceptos desarrollados por la neurociencia, los cuales no serán objeto de análisis en el presente trabajo, hacen parte de la simple mención de los estudios, que, sobre este campo, se adelantan y que involucran el derecho en materia penal y que en algún momento tendrán que abordarse con mayor claridad.

Para este caso, la mención de los diversos criterios de valoración del conocimiento y la voluntad, son necesarios en la determinación de la real o no voluntad del agente en la planificación y creación de los diversos sofismas de distracción que le permitan estafar a través de medios electrónicos, el punto de partida en esta nueva forma de estafa radica en el perjuicio que se ocasiona, sin embargo, para su penalización deben abordarse una serie de elementos, como hasta ahora, que nos permitan entender la necesidad de reconocerle como agravante de la conducta básica de estafa, a efectos de no incurrir en errores en la delimitación de la conducta.

2.5. El engaño concluyente. Un elemento a tener en cuenta.

Vistos todos estos elementos, debemos hacer un especial análisis a los que se conoce como el engaño concluyente, el cual parte de la base, de que al tratarse de un delito patrimonial y de comunicación, que contiene algunos presupuestos teóricos, en los que se deben analizar las nociones de engaño activo y de engaño por omisión, es pertinente mencionar que:

> El engaño concluyente es concebido como una forma de engaño activo, caracterizado por la necesidad de llevar a cabo un proceso deductivo del mensaje emitido y cuyo criterio son los elementos que definen la relación negociar de que se trate y sin los cuales esta dejaría de tener sentido. Además, el engaño concluyente es entendido como una afirmación falsa, implícita e indirecta, relativa a hechos típicamente relevantes. Definido el engaño concluyente en la estafa y planteados algunos de sus casos fundamentales. (Mayer, 2014, p. 1017)

La importancia de abordar este tema radica en la relación directa que tiene con la determinación de un componente necesario al momento de su realización como lo son las afirmaciones directas supuestamente hechas por las personas o empresas dueñas de la información

hurtada para la consumación del hecho. Es decir, en la ideación del acto, se muestra como ese paso de distracción sin el cual el sujeto activo de la acción no puede avanzar al siguiente nivel. Toda la estructura analizada párrafos atrás respecto del dolo, radican su centro en el aspecto de ideación de la actividad criminal, y este, el engaño concluyente, es la muestra de la necesaria explicación de las diversas formas de entendimiento del querer delictivo.

El concepto de engaño concluyente surgió de la expresión "perro muerto", utilizada en algunos países para identificar a quien se va, por ejemplo, de un restaurante sin pagar la cuenta. Según Díez – Picazo (1979):

> El concepto de "engaño concluyente" no se limita al tipo penal de estafa, pese a haber encontrado en él su máxima expresión. Es más, ni siquiera se circunscribe al Derecho Penal, pudiendo extenderse a toda relación comunicativa en la que sea posible construir una afirmación (falsa) mediante un proceso deductivo, afirmación que, por eso mismo, pasará a ser implícita e indirecta. Incluso más allá del concepto de engaño, el Derecho civil de los actos jurídicos reconoce ampliamente la posibilidad de emitir una declaración de voluntad a través de "actos concluyentes" (p. 104)

Es decir, se trata de un elemento que permite la intromisión a través de actos comunicativos en la ideación o consolidación del acto criminal, su consecución se centra en la maquinación de actos preparatorios falsos informados al sujeto pasivo quien asume como real lo que le es transmitido. Tradicionalmente se ha conocido al engaño (estafa), de acuerdo con la doctrina predominante sobre el tema, como un comportamiento activo en el que se lleva a cabo una puesta en escena (mise en scéne), en la que no solo se requiere una simple mentira, sino que para la consumación se hace necesario un hecho externo o material que le permita al sujeto activo consumar el acto delictivo.

Es pertinente, que se adviertan una serie de apariencias que le permiten al estafador manipular la realidad de quien se presenta como el sujeto pasivo. Es, en términos generales una etapa que se conoce como la maquinación o el ardid. Se concuerda con el Código Penal Español que el engaño debe tener la virtualidad de inducir en error. Se reitera, que no se trata de una simple mentira, la información emitida por parte del agente debe contener en sí, elementos que le permitan acceder a la información requerida para la consumación de su acto.

> Demandar un engaño bastante desplaza el foco del análisis, desde la representación a cargo del agente, propia de toda puesta en escena, hacía la reacción de cargo del disponente del patrimonio, pues precisamente respecto de dicha reacción el engaño ha de ser "bastante". Desde este punto de vista, la teoría de la mise en scéne desarrolla propiamente un concepto de engaño típico; la tesis del engaño bastante, en cambio, se ubica entre la conducta típica (engaño) y la reacción que esta tiene o puede tener (disposición patrimonial perjudicial determinada por error). Lo anterior, si bien puede fundamentarse en el carácter ambivalente de la noción de engaño, acarrea importantes complicaciones en la interpretación del tipo penal de estafa. (García, 2005, p. 23)

Ahora bien, en contraposición con la teoría de la puesta en escena, se debe decir que dentro de la legislación nacional en materia penal, no se exige para la consumación del hecho, que se ejecute este tipo de actos (mise en scéne), sin embargo, se reconoce que la manifestación de una simple mentira, como se ha mencionado, no configura en estricto sentido la estafa, por lo que para su consumación, se requiere de una serie de actuaciones que limitan la visión de la verdad del sujeto pasivo que lo sitúan en una condición que le impide conocer a ciencia cierta la realidad de la mentira que se le pone de presente para la consecución, en el caso de la estafa por medios electrónicos, de la información necesaria para la afectar su patrimonio.

El punto estructural de la estafa es la inducción al error, el cual se consolida a través del intercambio de información entre individuos, en el que uno actúa como agente con la clara intención de afectar el patrimonio de quien asume como real la información suministrada. No obstante, a los actos que debe realizar el agente, deben sumarse aquellos atribuibles al sujeto pasivo, en el entendido que la información que él suministre también debe ser de relevancia para que la relación negocial se perfeccione entre el estafador y él, con lo que termina configurándose un comportamiento patrimonial perjudicial a través de un engaño, y que de acuerdo con esto, se puede determinar que también se trata de un delito de autolesión, por supuesto, imputable a un agente.

2.5.1. El engaño activo y el engaño omisivo.

Ante todo, debemos partir por considerar que la acción en el engaño se traduce en la puesta en marcha de una actividad, bajo una afirmación falsa sobre determinados hechos, los cuales pretenden generar en el sujeto pasivo una distorsión de la realidad en permisión de las intenciones del agente, ello, como primer indicador del engaño activo. En este punto, quien realiza la transmisión de la información, lo hace con el pleno convencimiento que lo narrado constituye una realidad, disfrazada claro, pero necesaria en la consumación del acto, porque le permitirá, a través de la expectativa de veracidad, generar una recepción positiva en las intenciones.

La fuerza valorativa de lo narrado, esto es, de la afirmación lanzada, implica que se le reconozca o no como conducta típica, porque en ella radicará la posibilidad de generar consecuencias negativas en el patrimonio del receptor. Ahora bien, el engaño omisivo está sustentado, de acuerdo con Pastor (2004) en “la ausencia de una afirmación verdadera debida” (p. 43), es decir, en el ocultamiento de información necesaria en la comprobación de la realidad expuesta por el agente. Para los fines de la presente investigación, el engaño concluyente está

estructurado a partir de la acreditación de medios de convicción necesarios en el convencimiento del receptor, por supuesto relevantes para llevar a la consumación el hecho, por ello, la identificación de circunstancias activas o pasivas (omisivas) en el engaño, delimitan el grado de intervención del estafador a través de diversas formas de comunicación o del silencio, que también, como se mencionó, es una forma de consolidar el acto.

Algunos doctrinantes, consideran que no es acertado reconocer que el engaño concluyente es "una declaración sin palabras" (Tiedemann, 2012, p. 26), primero, porque en la manifestación de la voluntad del agente existe un intercambio de ellas (escritas o verbales), no necesarias, pero que llevan al convencimiento y segundo, porque, ante la no existencia de palabras, se torna un poco más difícil el intercambio de información necesaria para la afectación del patrimonio del receptor. El engaño concluyente es una forma más de comunicación, que no de ausencia de mensajes comunicativos de necesario entendimiento que permitan la accesión de la información. Con mayor razón debemos entender que en el caso de los delitos informáticos, el lenguaje utilizado, a pesar de ser mediante la utilización de plataformas, se torna mucho más específico y elaborado por la necesidad de llevar al convencimiento al sujeto en confiar en dicha información y por ende, acceder y vulnerar su patrimonio. Lo que sucede es que, en el engaño concluyente, no solo juega un papel importante los mensajes, porque de las diversas formas de comunicación se puede concluir que el agente con su actuar pretendió dar a entender una información alejada de la realidad, es decir, contiene en sí una intención explícita en obtener un beneficio a través del intercambio de datos. En términos generales, quien realiza un engaño concluyente, vulnera la norma y se convierte en sujeto activo de la acción criminal, lo sea por acción o por omisión, lo que, de acuerdo con la afectación del bien jurídicamente tutelado, constituye delito.

2.5.2. El proceso deductivo del engaño concluyente en la estafa.

El engaño concluyente, a través del proceso deductivo en el delito de estafa, depende de la afirmación falsa de una información que genere hechos típicamente relevantes, es decir, lo que provoca el engaño en la transmisión de información falsa que convence al receptor.

> Lo declarado (…) se ve contradicho lógica, empírica o normativamente por la ausencia de una circunstancia que, en cuanto presupuesto del sentido de la declaración, se entiende implícita en ella sin necesidad de mención expresa. En realidad, dicha forma de entender el engaño concluyente en el delito de estafa resulta equívoca y se vincula más bien con una noción general de aquello que es "concluyente". En la estafa, el disponente del patrimonio no realiza deducciones lógicas, empíricas o normativas, sino que conceptuales. (Hernández, 2010, p. 155)

La percepción que de la realidad asume el receptor está directamente ligada con la información suministrada por el sujeto activo, porque de ella es que nace la distorsión de la realidad y por supuesto la inducción al error con las consecuentes afectaciones patrimoniales. A través de los medios electrónicos se lleva al sujeto a la ideación de una realidad que para él es concluyente en cuanto es verdadera de acuerdo con lo mostrado por el agente. La realidad se torna verás con las actuaciones que se despliega y con la puesta en escena de una serie de manifestaciones inequívocas de la necesidad de obtener información sin la cual no se podría consumar el delito.

Ahora, el razonamiento que se espera del receptor de la información radica únicamente en entender y creer que efectivamente el despliegue de información por parte del agente es verdadero, que la puesta en escena se traduce en la comprobación de una realidad en la que se requiere la entrega de otra información necesaria para la consumación de un acto delictivo que generará a la

postré una afectación del patrimonio de quien se presenta como víctima. Es, sin duda, un acto que no permite, de manera fácil (menos con la utilización de medios electrónicos) identificar si efectivamente los argumentos expuestos son ciertos o no. La maquinación de la estafa concreta diversos factores en los que se pone de manifiesto el conocimiento y la astucia del sujeto activo en el convencimiento y manipulación de la información.

Todos estos elementos son de necesario estudio en la delimitación de las circunstancias que pueden rodear al delito de estafa y la concreta realización a través de medios electrónicos, porque nos permiten identificar sobre qué aspectos se debe sustentar o no la modificación del Código Penal respecto de los agravantes.

2.6. ¿Y, si en la estafa se utilizan medios electrónicos?

Hasta este punto hemos visto los diversos elementos que integran o mejor, que son necesarios en la consolidación o demostración del hecho delictivo denominado estafa. Sin embargo, y a pesar de reconocer que estos son de la esencia del delito, independientemente del mecanismo que se utilice, es importante analizar que sucede cuando en la ideación de la acción se involucran aspectos no tenidos en cuenta en la legislación nacional. Empecemos por manifestar que dentro de la descripción del artículo 246 y 247 del Código Penal, no se encuentra reconocido como mecanismo causal la realización del acto a través de medios electrónicos.

Ahora bien, a pesar de haber sido extenso el desarrollo de los elementos integradores del delito, se consideran de necesaria mención dadas las condiciones en el que se pretende plantear el asunto de la investigación. Porque, no solo se trata de mostrar una falencia normativa, sino la necesidad de evitar al máximo la indebida sanción penal con penas que no obedecen a los hechos jurídicos generadores de la acción penal. Es pertinente, desde esta óptica, tener claridad en que,

por principio de legalidad, las circunstancias que rodean el proceso penal deben preexistir a efectos no solo de garantizar los derechos del procesado, sino en últimas, generar seguridad jurídica frente a los actos que se investiguen. No obstante, este principio y su incidencia en la necesaria modificación del artículo 247 del Código Penal, será motivo de análisis en el capítulo 3 del presente trabajo investigativo.

Descendiendo al tema y a efectos de comprender de la mejor manera el asunto, debemos empezar por poner en contexto las situaciones que necesariamente convergen a la realización del delito de estafa cuando median aspectos tecnológicos en su realización.

Es cierto, para muchos, que, para la consumación del acto, se requiere únicamente la ideación a través de actos disuasorios que lleven al sujeto pasivo de la acción a creer en la mentira e incurrir en error. Sin embargo, no es tan sencillo el asunto, porque debemos tener en cuenta que dichos actos, en el contexto actual, dadas las nuevas modalidades de comercio electrónico, deben, en concepto de este trabajo, ser cobijadas, en el entendido que no debemos olvidar que este tipo de acciones criminales pueden surgir de diversas partes del mundo, pero, además, son múltiples las plataformas que pueden ser utilizadas para la consecución del fin.

A pesar de evolucionar en el manejo de mecanismos electrónicos, debemos dar por sentado que los cibercriminales son, por mucho, especialistas que se enfrentan a personas, que, en la mayoría de los casos no tienen la capacidad de reaccionar frente a las artimañas que se emplean para la comisión del delito. Normalmente, son tan elaborados los mecanismos de persuasión que no dan lugar a la distinción entre realidad y ficción. Este hecho es uno de los tantos indicadores que nos llevan a pensar en la posibilidad del reconocimiento de circunstancias que permitan, no solo desde la cuantía, imponer sanciones penales acordes con el perjuicio y la ideación del hecho delictivo. Actualmente, las circunstancias de agravación punitiva contempladas en el artículo 247

del Código Penal, no permiten encasillar estos elementos como generadores importantes del engaño.

De hecho, no aportan en la consolidación o establecimiento de la sanción y determinación del delito. Ahora, si de lo que se trata es de hacer frente a estas nuevas formas de criminalidad, crecientes día a día, y a proteger mecanismos de comercio que se rigen en mayor medida a través de medios electrónicos, debería ser punto de partida, el reconocer dentro de la legislación aspectos de suma importancia como lo son estos, ya que podemos caer, como en efecto sucede, en la pérdida de efectividad de la intención preventiva del derecho penal.

No se busca, el endurecimiento de las penas porque sí, es la evolución del derecho lo que se pretende con el reconocimiento de figuras o elementos que juegan un papel determinante actual en la comisión del delito. Seguramente, hace 30 o 40 años no sería relevante establecer este tipo de agravantes porque en términos generales para esa época el comercio electrónico carecía de los participantes actuales. Es inminente el crecimiento de plataformas que prestan servicios financieros de toda índole, y por ello, la responsabilidad del estado debe radicar en la intervención efectiva de diversos mecanismos que entiendan y comprendan las nuevas realidades sociales. No por nada, en otras ramas, como la laboral, se ha permitido, a través de desarrollos tecnológicos, realizar las funciones desde los sitios de residencia.

Es de tal trascendencia esta modificación pretendida, que actualmente, en la Sala de Casación Penal de la Corte Suprema de Justicia, no existen antecedentes respecto a la comisión del delito de estafa cometido a través de medios electrónicos y no porque no se hayan presentado, sino porque, seguramente la existencia de este tipo de elementos en la consumación del delito no es estudiada.

Y es que, los avances legislativos al respecto han sido bastante pocos, entendiendo los esfuerzos que se han adelantado para reconocer algunas de estas especiales formas de criminalidad, pero los cuales no han sido contundentes, por lo menos en lo que respecta a la presente investigación.

Miremos, cómo la Ley 1928 de 2018 que introdujo en el ordenamiento interno el Convenio de Budapest relativo a la Ciberdelincuencia, permitió, consolidar los lineamientos trazados a partir de la Ley 1273 de 2009 la cual creó el Título VII Bis del Código Penal Colombiano, relacionado con la protección de la información y de los datos, generó una modificación importante en cuanto al establecimiento de herramientas que hicieron visibles las nuevas de ciberdelincuencia. Sin embargo, y a pesar de contener de manera general una real aproximación en la intención de protección de los usuarios de las redes, no generó un total reconocimiento de las diversas formas delictivas.

Es así como, en dicho título, y relacionados con aquellos cometidos con el patrimonio económico, estableció unos tipos penales para hacer frente a situaciones en las que, por ejemplo, con la intención de hurtar, se utilizan herramientas tecnológicas. La intención, por supuesto que es buena, importante, pero no completa. Nótese, que este bien jurídicamente tutelado se mueve en diversos aspectos de la propiedad del sujeto pasivo. En él, se pretende la protección de sus bienes más próximos cuantificables en dinero. El hurto, en sus diversas acciones quedó protegido y que sucedió con la estafa. El punto, de acuerdo con la lectura del tipo penal del 246, queda desprotegido en una de sus formas actuales más recurrentes. ¿Por qué?, porque no es posible atribuirle responsabilidad de un delito llevado a cabo con medios tecnológicos a quien lo realiza. Se parte de un supuesto básico, simple, que no guarda relación con el principio de taxatividad de la norma penal.

Si ello es así, se entra en un vacío que no tiene forma de protección, porque de allí, es decir, de un delito como estos, en cuanto a estafa, solo se puede permitir como posible el agravante que la misma descripción del tipo contiene por la cuantía. Y es que acaso, la utilización de medios especiales para la consumación del acto, ¿no son de importancia y valorables en la aplicación de la sanción penal?

Nótese, que, en el caso del hurto, se cobijan diversos mecanismos que puedan llegar a ser utilizados en la comisión del mismo, al punto, que existe, dentro de las categorías del delito, el hurto calificado y agravado. Este reconocimiento permite, de manera directa, evitar diversas interpretaciones en cuanto a aplicación de la ley penal. Sin embargo, en el evento de la estafa, por más que se utilicen medios especializados electrónicos en la realización del acto, estos pasan desapercibidos porque no son del resorte de la ley penal, o por lo menos así está establecido en el código.

Podrán, ser utilizados como medios probatorios, pero el mecanismo o mecanismos quedan desprovistos de intervención y por ende de sanción penal. Lo sorprendente del asunto, es que cuando se analizó y estudió el proyecto de Ley 042 de Cámara, 123 Cámara y Senado acumulados, se hizo especial mención a la intención de asumir políticas penales globalizadas en materia de combate frontal contra este tipo de criminalidad. Todas, en todas sus formas, es decir, cualquier tipo de criminalidad que utilice como mecanismo medios electrónicos. La realidad nos arroja a un vacío en el que convergen normas cercanas de imposible aplicación por expresa prohibición de analogía en el mundo penal.

Uno de los aspectos más importantes del Convenio de Budapest, fue el reconocer componentes de cooperación internacional que hacen evidente la creciente ola de ciberdelitos, y la necesidad de cerrarle las puertas desde cualquier punto susceptible de vulneración de los

delincuentes. No obstante, son bastante los vacíos, o por lo menos en cuanto a estafa se refiere, dadas las circunstancias narradas hasta aquí.

Todos los elementos mostrados nos sirven de un sustento necesario en la estructuración pretendida a partir del capítulo 3 de la presente investigación, en el que, entre otros aspectos se analizará, lo relacionado con el principio de legalidad como pilar fundamental en la necesidad de incorporar en el ordenamiento jurídico el agravante mencionado en el artículo 247 del Código Penal. Ello, como respuesta necesaria a la creciente criminalidad de los ciberdelitos y a efectos de no permitir que estos mecanismos no queden desprovistos de intervención penal.

Conclusiones Capítulo II

- A pesar de los esfuerzos, como sucede con la Ley 1273 de 2009, en dichos mecanismos no se hace referencia a temas como lo son los ciberdelincuentes en el delito de estafa, dejando así una brecha muy importante dentro de la legislación Penal Colombiana.

- El derecho penal en Colombia tiene una tarea maratónica y es la de regularizar todos los adelantos tecnológicos a los que tienen acceso los ciberdelincuentes, a efectos de individualizar conductas que desde todas las ópticas ocasionen daños en materia económica. Es necesario entender que dichas acciones se pueden realizar desde cualquier lugar, lo que imprime un trabajo mucho más difícil de consolidar, pero no imposible. Es importante articular de manera adecuada, conjunta y global, las intenciones de persecución para poder perseguir y capturar los ciberdelincuentes que utilizan la web como instrumento de la criminalidad.

- Debemos tener presente que para poder combatir y disminuir la brecha tan importante que existe en nuestra legislación Colombiana para judicializar a las personas que incurran en este delito de la ciberestafa, necesitamos que se cree una excelente unión, participación y colaboración de todos los entes del Estado Colombiano encargado de combatir estos cibercrímenes, como lo son la Policía Nacional, la Fiscalía General de la Nación e inteligencia del Ejecito Nacional, entre otras, para así y de esta manera lograr un frente de batalla inigualable en contra de este flagelo.

- Existen, en los diversos planteamientos expuestos en este capítulo, aspectos de suma importancia en la demostración de una necesidad que está orientada a la modificación de la legislación penal Nacional, con respecto a los agravantes de la conducta de estafa. Sin embargo, era necesario mostrar la realidad y los elementos que estructuran el delito y que hacen parte de la

esencia misma de éste, para consolidar una modificación de suma importancia y a la par conocer como ha venido evolucionado el concepto y de qué manera se aplica en nuestro sistema normativo.

- Un análisis importante en la materialización del acto se encuentra en poder determinar, de qué manera el sujeto activo de la acción puede intervenir y aportar en la consumación del acto. Ello, hace parte del estudio de las formas en que se puede mostrar el delito desde su ideación hasta su culminación. Surge, entonces, importante conocer, debido a la constante evolución de los medios electrónicos utilizados y a la profesionalización de los delincuentes, el cómo se utilizan mecanismos persuasivos que permiten vulnerar la intencionalidad del receptor en la consecución de la información necesaria para proceder a la estafa.

- No es un tema de simple valoración subjetiva, ya que, de acuerdo con lo visto, los instrumentos de engaño son mayores a los de protección y en ese orden de ideas debemos orientar los esfuerzos en la ideación y planeación de mecanismos preventivos. Para ello, se reitera, es importante conocer a fondo, todos y cada uno de los elementos integradores del tipo penal denominado estafa y así entender y comprender cómo se puede hacer frente a los nuevos métodos utilizados para su consumación.

- La exigencia en este capítulo fue identificar puntos de vista poco conocidos para entender de la mejor manera, porqué en el delito de estafa, también se puede hablar de omisión con las consecuencias nefastas, todo en orden al patrimonio. Los actos comunes en este delito son mucho más amplios de lo pensado, por ende, el reto del siguiente capítulo radica en la articulación de toda la información recopilada para entender y establecer la hoja de ruta que permita pensar de manera concreta en la modificación del Código Penal en lo que respecta a los agravantes en este delito, ello como respuesta necesaria a su constante evolución.

CAPÍTULO III: El Ciberdelito. La necesaria modificación del artículo 247 del Código Penal.

Hasta aquí, la investigación se ha centrado en aportar elementos que nos permitan desarrollar en estricto sentido la teoría central de lo que se quiere demostrar. Son, hasta ahora, hechos que nos muestran diversos fenómenos criminales y diversas realidades sociales que nos arrojan a un mar de posibilidades delictivas, todas, diferentes unas de otras, pero en últimas, generadoras de perjuicios. La diversidad social es cada día mayor y en ese sentido nos hace enfrentar nuevos retos en materia penal. Somos, todos, testigos del ingenio y creatividad de los delincuentes en crear mecanismos de engaño que llevan a incautos a perder su dinero o diversos bienes.

La labor del Estado en ese sentido, se encuentra en la necesidad implacable de buscar nuevos medios de seguridad que permitan hacer un frente común en búsqueda de disminuir los riesgos en el uso de nuevas tecnologías. Pero, nada de esto puede ser posible si no se crean las leyes y políticas que nos permitan actuar diligentemente. Claro, en materia penal, el tema es un poco más complicado por las mismas exigencias normativas. De hecho el artículo 6 de nuestro Código Penal Colombiano, impone una exigencia de estricto cumplimiento, el principio de legalidad, el cual se presenta como ese elemento de imposible inobservancia, ya que al ser un principio de la esencia del proceso penal, no puede ser pasado por alto.

A continuación, y para concluir esta investigación, se demostrará, porqué, a pesar de existir mecanismos de lucha contra la criminalidad, se debe reconocer como agravante dentro del delito de estafa, a aquellas cometidas por medios electrónicos, atendiendo precisamente los postulados del principio de legalidad, ante la imposibilidad, de juzgar a quien hasta este momento incurra en

esta conducta, por no estar enmarcada dentro de la legislación penal, por lo menos en búsqueda de una sanción más fuerte.

3.1. El Principio de Legalidad.

Uno de los aspectos más importantes en el surgimiento del principio de legalidad precisamente se encuentra en la necesidad de imponer un control al poder punitivo del Estado y tratar de evitar de esta manera arbitrariedades y por supuesto brindar herramientas a quien, independiente de la razón, se sometiera a la justicia penal. Uno de los antecedentes más importantes lo encontramos en la Declaración de Derechos de Virginia de 1776, en cuanto que su artículo 8, prohibió la privación de la libertad sino en virtud de las leyes de cada Estado.

Beccaria (2015), al abordar el tema, mencionó que, “la primera consecuencia de estos principios es que solo las leyes pueden decretar las penas de los delitos, y esta autoridad debe residir únicamente en el legislador que representa toda la sociedad unida por el contrato social. (p. 21). Lo que implica, que no puede, en materia penal, existir un proceso en el que se juzgue sin que la misma ley lo reconozca como tal y por supuesto que imponga su pena. Es preciso indicar que el principio de legalidad no solo implica la prexistencia de la norma en materia penal, éste, se erige como un pilar en la necesidad de crear normas claras, de lenguaje común y entendibles para la sociedad, ello, también es un límite al poder punitivo del estado, en tanto que, cuanto mas clara la norma, menor la probabilidad de arbitrariedad de los operadores de justicia.

Tiene que entenderse que la ley penal debe constituirse como la mayor garantía del limite a los poderes del estado, en razón a la implicación que tienen el tipo de sanciones que aquí se imponen. Cierto es, como lo mencionó en su momento Filangieri, que las buenas leyes son la clave para conservación y el progreso de la sociedad, sin estas, estaremos destinados al fracaso ante la

imposibilidad de brindar seguridad a nuestros asociados. Seguridad que no se circunscribe únicamente a la protección de los peligrosos, de los delincuentes, sino a brindar en términos reales a todos por igual, las mismas condiciones en el proceso penal.

El principal desarrollo del principio de legalidad por nosotros conocido se hizo visible a través del concepto *nullum crimen nulla poena sine lege*, que introdujo en nuestro lenguaje jurídico la concepción respecto de la imposibilidad de existir sanción sin que medie una ley que así la reconozca. Diversos autores han aportado en el entendimiento y mejor análisis de este concepto, tal vez, y no solo a criterio propio, Feuerbach (2010), se constituyó como el pionero de la construcción del concepto del principio de legalidad, si tenemos en cuenta que para él, la tarea fundamental del Estado es la realización material de la Constitución, del conjunto de leyes fundamentales sobre las cuales se construye la sociedad civil organizada en procura del aseguramiento recíproco de las libertades de todos. (p. 76.)

Nótese que la intención vista en la diversas etapas del pensamiento del derecho penal, se centran en la posibilidad de imponer al Estado límites a su ejercicio punitivo, a efectos de evitar las arbitrariedades del pasado, no podemos olvidar que estos límites son y han sido una exigencia social, en cuanto representan la lucha constante de quienes pretendieron y pretenden la evitación de menoscabos sociales por parte de los estados. Paradójicamente, las leyes penales son garantía de las libertades individuales en tanto que reconocen aquellas que atentan precisamente contra estas libertades y además porque imponen o deben reconocer de manera clara y precisa la manera en cómo se debe imponer el castigo para quien viole dichas libertades.

En ese sentido, lo que se busca es que se identifiquen esas especificidades de cada situación social y desde allí se determine la sanción. Es claro que ante la inexistencia normativa, no puede actuarse de manera diligente, porque la ley precisamente debe reconocer esos parámetros dentro

de los cuales el Estado debe moverse y cumplir de manera estricta dicha función. La preexistencia de los tipos penales son presupuestos indispensables para ejercicio del *ius puniendi*, sin ellos el operador judicial incurre en arbitrariedad, la necesidad de reconocer los diversos elementos delictivos en la ley, radica precisamente en la posibilidad de entender y comprender los cambios sociales y garantizar, incluso al delincuente, que se actúa con transparencia y convencidos que a quien se juzga por un delito se hace con el convencimiento de que su conducta constituye delito, de lo contrario, podrían, los fines esenciales del Estado, caer en vacíos legislativos que en materia penal no pueden ni deben existir.

La rigurosidad del derecho penal no da posibilidad de maniobras como sucede en otras ramas del derecho. Por ello, aquí no es posible hablar de analogías, en este campo la exigencia es mucho mayor y por ende, ni siquiera en aplicación de la *secundum legem* se puede llegar a acudir a normas concordantes para definir si esta puede ser considerada como delito. Diversos autores consideran de manera acertada que la ley penal es expresión de libertad, igualdad y seguridad, "orientadas a la búsqueda de la felicidad como criterio de racionalidad en su primer nivel de significación" (Grosso, 2019, p. 99)

La ley penal, en su concepción implica el reconocimiento de principios de igualdad, es decir, debe ser aplicada a fin de garantizar la libertad de la sociedad y también a efectos de que se garanticen en los mismos términos los derechos de quienes asumen como posible la violación de las normas, del rompimiento de aquel contrato social que tanto nos habló Rousseau. Más aún, se constituye en un concepto de importancia superior en cuanto a seguridad, no como aquella relativa de manera subjetiva a los individuos de manera individual o colectiva, sino aquella que cobija el estado de cosas expresadas en términos de seguridad jurídica, de una sociedad que se enfrenta al

poder del Estado a través de la ley, confiada en que el derecho de ninguna manera violentará los derechos ni las libertades aquí tantas veces mencionados.

Líneas atrás se mencionó el concepto del profesor Grosso en cuanto a que la ley penal busca la felicidad. Pues, fíjense que precisamente el garantizar, en las diversas categorías, las libertades de los ciudadanos implica dicho fin, por ende, el Estado, a través de la norma solo puede prohibir y castigar aquellas que atentan contra las libertades públicas y por ende se encuentra obligado a regularlas a través de la ley, precisamente en atención al principio de legalidad. La ley, en este sentido, se erige como una exigencia de regular conductas futuras que puedan ser generadoras de perjuicio social, por tal motivo no puede pensarse en sancionar conductas que no estén expresamente prohibidas y sancionables a través de la norma penal.

3.2. La necesidad del principio de legalidad en materia penal.

Claramente se ha dicho que en materia penal, el principio de legalidad constituye una herramienta de gran importancia en cuanto limita el poder punitivo del Estado. Pero, es importante resaltar que este principio no solo se traslada a los ámbitos del proceso como tal. También impone una obligatoriedad en cuanto al órgano encargado de crear la ley. Porqué?, por que es él quien debe velar por que las conductas generadoras de perjuicio social deban ser reconocidas como delito. Este hecho se conoce como criterio negativo del principio, ya que implica que quien tiene el deber al no hacerlo puede generar problemas de seguridad jurídica que a la postre conducen a situaciones de impunidad al no poderse juzgar a quien cometa un delito.

Una de las razones de la presente investigación es la de hacer evidentes estos elementos, todos, absolutamente todos, sirven en la construcción de las bases requeridas para la identificación de la necesidad de reconocer como posibles y sancionables conductas que hoy no pueden ser

intervenidas por la ley penal, por el simple hecho de no estar así reconocidas. El principio de legalidad, así las cosas, es un presupuesto no de la ley penal, sino de su formación, en tanto que debe manifestarse en un hecho jurídico el cual conocemos como delito y su consecuente sanción. Si ello es así, éste nos debe servir para fomentar positivamente la creación o modificación de leyes existentes que entiendan las nuevas formas de criminalidad.

El reconocimiento de estas diversas formas surge por necesidad, orientadas por la evolución social, y precisamente por la imperiosa obligación de reconocer que surgen nuevos sistemas delictivos. En este sentido, no puede el derecho penal, quedar al margen de estas nuevas realidades, porque de ser así, se entraría en una peligrosa anomia que impediría de manera directa, como en efecto sucede, que no se puedan investigar delitos por su misma naturaleza. Estas modificaciones son de inminente reconocimiento, pues, son mecanismos de reforzamiento normativo frente a los nuevos desafíos. Bien es sabido que el derecho penal no puede funcionar sin las herramientas básicas que le permitan actuar de manera real ante dichos cambios, ello, es precisamente lo que justifica la existencia del derecho penal.

Lo que se busca es que no se acuda a los vacíos normativos para generar impunidad. El criminal siempre está aleta en la identificación de ellos como fuente precisamente de su actuar criminal. Un vacío, es, sin duda, un paso hacia una injusticia que por obvias razones quedaría huérfana de sanción penal. Las libertades de los ciudadanos en cualquier escenario deben ser protegidos, cualquier ataque, independiente de su mecanismo debe y tiene que ser repelido por quien espera la sociedad que actúe.

> Las normas penales son las herramientas semánticas que viabilizan el dialogo entre ciudadanos que se reconocen mutuamente como iguales y que se valen del lenguaje del derecho penal para ponerse de acuerdo en aquello que ellos no quieren que suceda, pero

> que, sabedores que va a suceder, establecen de antemano y por consenso las pautas de respuesta para esos eventos, justamente para que su producción no afecte de tal manera a la comunidad de hablantes que rompa el diálogo; de esta manera, la pena es el instrumento que asegura que el diálogo continuará aun a pesar de que alguno de los dialogantes inobservó las pautas dentro de las cuales se había establecido y asegura también que se lo siga considerando incorporado a la sociedad y se insiste en que observe las normas. (Grosso, 2019, p. 837)

Lo que se busca significar con estos elementos, es la necesidad de reconocer los diversos mecanismos delictivos y así garantizar el goce de las libertades de los ciudadanos en sus diversas formas de interacción social, finalmente, se pretende es la evitación del menoscabo de los derechos ciudadanos y este solo se logra si efectivamente es posible perseguir la criminalidad desde todas las vertientes. En esta materia no se trata de crear normas sin ningún sustento, cayendo a extralimitaciones legislativas, no, aquí lo que se pretende es la efectiva identificación de todos y cada uno de los dispositivos que puedan llegar a ser utilizados en la comisión de delitos.

3.2.1. La necesidad de una ley penal compuesta.

Bien sabido es que para que una conducta sea considerada como delito, no solo debe verificarse la producción de un daño, ésta, debe estar rodeada de factores de entidad suficiente que sean importantes para el desarrollo del delito. Si esto es así, también lo es que el reconocimiento de estas condiciones implican que en grado alto puedan ser investigadas y por ende generen una sanción para quien asumió la infracción. El reconocimiento de todos y cada uno de los elementos integrantes del delito no es un mero capricho, en nuestra legislación se ha entendido la necesidad de abordar diversos mecanismos delictivos y su determinación se ha hecho pertinente a efectos de generar diferentes tipos de sanción, entendiendo la intención y mecanismos de realización.

Las conductas así descritas logran una mejor comprensión y tratan de evitar al máximo incurrir en indebidas interpretaciones de la ley penal. Ante la claridad de la norma es evitable en mayor grado que el operador judicial opte por aplicar indebidamente tipos en el que no concurran las características del efectivamente cometido. Ahora, si lo que se pretende es que se evite al máximo incurrir en error, con mayor razón se debe, en atención al principio de legalidad, reconocer las diversas modalidades del delito. El criminal sabe de derecho penal, por una sencilla razón, es en él en quien a la postre recae la sanción. Es por ello que a la par del crecimiento de la sociedad, surgen nuevas modalidades de delito, la labor, como muchas veces se ha mencionado, consiste en avanzar al mismo ritmo, al margen de quienes, estamos seguros, conocen los vacíos normativos y la imposibilidad, por lo menos en materia penal, de que sin ley preexistente puedan ser sujetos de intervención y sanción.

No basta con mencionar dentro del tipo penal el bien jurídicamente tutelado, se requiere además, como sucede en diversos delitos, que estén integrados al mismo, como agravantes, aquellos elementos con los que se consuma el daño. Es claro que dependiendo de los mecanismos utilizados se puede lograr o materializar en mayor medida la consumación del hecho. En delitos como el hurto, establecido en el artículo 239 del Código Penal y debido a las diversas formas en como se presentaron algunos actos delictivos, se hizo necesario incluir como agravante aquel cometido por persona disfrazada (art. 241 numeral 4) o en lugar despoblado (art. 241 numeral 9). La intención de que estos tipos penales sean complementados de esta manera, simplemente se encuentra en la necesidad de reconocer la pericia del delincuente en querer ejecutar y consumar el hecho delictivo.

No puede ser sancionado de la misma manera aquel que por una circunstancia simple decida hurtar un celular, a quien, acudiendo a algunas artimañas, decida realizar la misma

conducta. En el segundo caso, se está ante la manipulación e imperiosa necesidad del delincuente de culminar o consumar su hecho a toda costa. Estos elementos, por supuesto no pueden ser desconocidos, son mecanismos que deben ser valorados al momento de imponerse la sanción y el no estar reconocidos en la ley penal, deja desprovisto de herramientas al operador judicial y por ende, desconoce la intención en la materialización del hecho. Son situaciones que de no estar reconocidas quedan desprovistas de intervención por parte del estado y por supuesto, a la postre impunes.

3.2.2. La utilidad de la ley penal.

Un aspecto de relevante importancia en el reconocimiento de tipos penales que aborden todos y cada uno de los aspectos que entran en juego en la comisión del delito, es la utilidad que el mismo genere en la sociedad. Recordemos que existe una necesidad de encontrar la felicidad a través de los fines del estado, y en ese sentido, dicha felicidad se encuentra amarrada a la mayor o menor posibilidad de materialización de las libertades sociales. Es decir, a mayor probabilidad mayor será el éxito de la norma penal, porque puede evitar que esas libertades sean menoscabadas.

De acuerdo con Grosso (2019),

> El principio de utilidad pone en evidencia la necesidad de un radical cambio estratégico respecto de la perspectiva desde la cual se hace el análisis y se planifica la criminalización de las conductas, que se suele enfocar en la desviación como hecho que se da por sentado y como objetivo a superar. (p. 865)

El objetivo de la norma penal debe estar sustentado en tratar de abordar el mayor campo posible, entendiendo que por exigencia del principio de legalidad y nuestro artículo 6 del Código Penal, solo es sancionable aquellas conductas que se encuentren tipificadas como tales y en ese

sentido debemos tener certeza que ante situaciones de anomia no solo en el tipo autónomo sino en sus agravantes, algunas circunstancias sancionables pudieran quedar en la impunidad. No solo se trata de desbordar el código con normas innecesarias, se trata de evolucionar a la misma velocidad de la sociedad, cuanto más robusto sea nuestro sistema penal, mayor probabilidad de alcanzar la felicidad y por supuesto la aplicación de la sanción. El reconocimiento dentro de la ley penal de diversas herramientas criminales busca en alguna medida poner trabas a los delincuentes, es un mecanismo preventivo si se quiere, pero a la postre se torna en un instrumento de evitación de una no sanción. Todas, absolutamente todas las formas de criminalidad deben ser sancionadas y por ello se han tipificado diversas herramientas delictivas en los conocidos agravantes de las conductas.

Así las cosas, el camino no es otro que el de reformar la ley basado en la necesidad y utilidad de la ley penal, pero teniendo como estructura siempre la exigencia del cumplimiento y acatamiento al principio de legalidad. Esto no quiere decir que las normas deban ser reformadas a diario o que las mismas deban ser creadas de manera provisional, sin embargo, lo que se pretende es que se reconozcan todos y cada uno de los elementos que pueden confluir en la comisión del delito y desde allí generar la posibilidad de ser sancionado. Lo que se busca con este tipo de reformas es que las decisiones que se tomen por parte de los operadores judiciales sean correctas y en la mayor medida posible justas, con ello se garantiza la seguridad jurídica.

Los elementos aquí descritos en cuanto necesidad y utilidad de la ley penal, se encuentran relacionados directamente con la Constitución Política (1191), de hecho el artículo 28 impone:

> Toda persona es libre. Nadie puede ser molestado en su persona o familia, ni reducido a prisión o arresto, ni detenido, ni su domicilio registrado, sino en virtud de mandamiento

> escrito de autoridad judicial competente, con las formalidades legales y **por motivo previamente definido en la ley**. (negrilla fuera del texto)
>
> La persona detenida preventivamente será puesta a disposición del juez competente dentro de las treinta y seis horas siguientes, para que éste adopte la decisión correspondiente en el término que establezca la ley.
>
> En ningún caso podrá haber detención, prisión ni arresto por deudas, ni penas y medidas de seguridad imprescriptibles.

Es evidente que la necesidad de reconocer dentro de los tipos penales cualquier herramienta utilizada en la comisión del delito como elemento necesario en su consumación y por ende de suma importancia al momento de imponerse la sanción, no desciende únicamente de nuestro Código Penal, es la misma Constitución la que nos obliga a la definición previa de todas las formas de criminalidad. Su contenido y finalidad, expresan la voluntad impuesta por la norma superior y desde allí debe impactar a todo el ordenamiento jurídico, por supuesto no solo al penal.

Así las cosas y al ser una voluntad del pueblo plasmada en la norma superior, debe el legislador ceñirse estrictamente a las necesidades de la sociedad, en cuanto que es ella, la sociedad, las directas víctimas del cambiante mundo de la criminalidad. El no hacerlo, es una muestra de la falta de intervención del estado en la lucha contra esta. La protección a los ciudadanos empieza desde la constricción de políticas criminales adecuadas que brinden a los operadores judiciales las herramientas para enfrentar los diversos métodos utilizados en la comisión del delito. Esta es la muestra que las instituciones funcionan articuladamente entendiendo nuestra realidad, una realidad, que como veremos trasciendo al mundo de lo virtual, de lo electrónico, de las tecnologías y el derecho, más concretamente el penal no puede quedarse atrás sin evolucionar reconociendo

las nuevas modalidades de delito, en donde las herramientas utilizadas por los criminales juegan un papel importante en la consumación del mismo y por tal deben ser sujeto de mayor responsabilidad y sanción penal.

3.3. Una necesaria modificación del artículo 247 del Código Penal.

La estructura y elementos integrantes del delito de estafa fueron abordados ampliamente en el Capítulo II de la presente investigación. En él se hizo especial énfasis en su contenido, empezando el 3er capítulo se mostró la necesidad de reformar o ampliar los agravantes, a efectos de generar un mayor campo de aplicación en cuanto a los elementos que pueden concurrir en la comisión del delito.

El Código Penal, en su artículo 247, establece:

> Circunstancias de agravación punitiva. La pena prevista en el artículo anterior será de sesenta y cuatro (64) a ciento cuarenta y cuatro (144) meses cuando:
>
> 1. El medio fraudulento utilizado tenga relación con vivienda de interés social.
>
> 2. El provecho ilícito se obtenga por quien sin ser partícipe de un delito de secuestro o extorsión, con ocasión del mismo, induzca o mantenga a otro en error.
>
> 3. Se invoquen influencias reales o simuladas con el pretexto o con el fin de obtener de un servidor público un beneficio en asunto que éste se encuentre conociendo o haya de conocer.
>
> 4. La conducta esté relacionada con contratos de seguros o con transacciones sobre vehículos automotores.

5. La conducta relacionada con bienes pertenecientes a empresas o instituciones en que el Estado tenga la totalidad o la mayor parte, o recibidos a cualquier título de este.

6. La conducta tenga relación con el Sistema General de Seguridad Social Integral.

Nótese que en ningún aparte se reconoce la realidad mostrada en los capítulos anteriores, es decir, la creciente criminalidad a través de medios electrónicos. De hecho, en otros tipos penales si se sanciona aquellas conductas cometidas a través de estos, como se evidencia en el artículo 269I, hurto por medios informáticos y semejantes. Es decir, se permite y se entiende que a medida que la sociedad evoluciona en temas mercantiles, comerciales, también evolucionan los mecanismos con que los criminales cometen sus delitos. En algunos aspectos del Código Penal, el legislador si ha entendido la necesidad de, atendiendo el principio de utilidad, ampliar la norma reconociendo estas circunstancias. No es un capricho innecesario, es una imposición legal, es una necesidad proteccionista frente a nuevas realidades.

Los usuarios de la internet, que en la actualidad somos muchos, casi todos a nivel mundial, estamos expuestos a diversos mecanismos de fraude, de hurto y de engaño, cada una de estas modalidades incluye un sistema de distracción o consumación diferente, el cual, pretende en la mayor medida posible la consumación del hecho. Y es que los delincuentes cada día asumen nuevas herramientas de profesionalización que les ha permitido en gran medida la realización del delito. El problema radica en la consolidación no solo de mecanismos preventivos en la internet sino en el establecimiento de políticas penales que refuercen los tipos penales actuales y sus agravantes como en el caso del hurto, a efectos de poder imponer las sanciones acordes a la infracción. No hablamos solamente de castigar, sino de imponer la sanción que efectivamente se adecue a la conducta cometida y a las estrategias implementadas para ello.

Debemos entender que al ser un tipo penal autónomo, la estafa cometida a través de medios electrónicos no puede equipararse al del hurto establecido en el artículo 269I, puesto que ambos contienen una estructura diferente y los móviles, así el fin perseguido sea similar, se contraponen a la forma en como cada uno se lleva a cabo.

En ese sentido, no puede el operador judicial, sustentado en la extracción, por ejemplo de dinero, asumir que por alcanzarse el mismo bien, trasladar la conducta a la que se asimile a la afectación del bien jurídicamente tutelado, que para el caso de la estafa y el hurto son el mismo. En materia penal esa remisión no es posible, recordemos que la analogía no es aplicable en esta materia, por lo que ante la inexistencia de reglamentación al respecto, la modalidad delictiva queda o puede quedar impune.

No existe forma de equiparar las conductas por el hecho de perseguir fines patrimoniales, porque en el hurto la perdida del bien patrimonial se da en contra de nuestra voluntad, en ese momento nos encontramos en pleno uso de nuestra razón y conciencia, mientras que en la estafa, entregamos voluntariamente el bien u objeto, debido al engaño planeado por el delincuente.

Ahora, mas allá de ser evidentes estas diferencias, en la práctica, se escuchan algunas voces de operadores judiciales para quienes el fin perseguido por el delincuente permite llevar a cabo la investigación a través de la conducta reconocida en el artículo 269I, situación que a criterio propio genera una gran problemática y atenta contra el principio de legalidad, en el entendido que son tipos penales autónomos con un desarrollo estructural bastante amplio que no permite un entremezclamiento caprichoso y amañado so pretexto de aplicar justicia.

Para la presente investigación, se hace evidente que en el artículo 247 de los agravantes del delito de estafa, no se introdujo como sancionable aquella cometida a través de medios

tecnológicos y ello implica que por más grave que sea la estafa, por más que las artimañas utilizadas trasciendan al mundo de la internet, por más que se hayan implementado sistemas novedosos de engaño, deben y tienen que ser considerados como una simple estafa sin la posibilidad de imponer, por ese hecho una sanción mayor. Aquel servidor judicial que pretenda hacer una valoración jurídica diferente, en concepto propio, no solo incurre en una arbitrariedad sino que podría caer en el campo del derecho penal, en vista de que aquí no es posible permitirse atribuciones legales que no se encuentran enmarcadas en la ley.

La estafa como se encuentra actualmente tipificada no cobija ni tiene prevista una sanción especial para aquellas conductas en las que se utilicen medios electrónicos, lo que implica no solo la falta de poder punitivo del estado en ciertos casos, sino la posibilidad de que la delincuencia avance en la profesionalización del delito sin ningún tipo de control, finalmente, una sanción mínima de 32 de meses independientemente del daño o perjuicio económico es realmente poco.

Por estas razones es que se considera muy necesario que se avance en la modificación de la ley penal en este sentido, los mecanismos preventivos y las herramientas de seguimiento a los ciberdelincuentes deben tener como estructura una normativa sólida, completa y compleja que permita el adecuado accionar de las entidades del estado. Estamos avanzando con grandes pasos a la consolidación de medios de trabajo sin la intervención presencial del ser humano, se está evolucionando en sistemas de teletrabajo, los medios informáticos abarcan cada día más espacio en nuestras vidas. Las transacciones electrónicas se han trasladados al celular y estos vacíos legales lo único que hacen son brindar herramientas a los delincuentes y dejar al descubierto a millones de incautos cada día.

Es necesario, dar un paso en este sentido y buscar a toda costa el reconocimiento de esta modalidad delictiva de la estafa, debido no solo a su falta de reglamentación, sino atendiendo la

evolución de la sociedad y su migración a la vida digital. El camino es largo y seguramente se encontrarán voces en contrario, pero la evidencia normativa y social nos muestra un camino desprovisto de protección por parte del estado para quienes nos enfrentamos a un mundo digital plagado de delincuentes a la espera que alguien caiga en sus redes de manipulación y se convierta en una victima más de los ciberdelincuentes. Ojalá el tiempo nos de razón y nos permita ser testigos de la transformación de la ley penal en beneficio de la sociedad en el que se asumen y reconocen estos nuevos retos. Espero, sea así.

Conclusiones Capítulo III

- Para que una sociedad evolucione de manera positiva debe permitir que sus normas lo hagan en el mismo sentido. Es decir, que entiendan las nuevas realidades y allí deben estar contenidas aquellas que se ajusten a las nuevas modalidades de delito como respuesta necesaria que le permita a los operadores judiciales actuar en debida forma con el convencimiento que cuentan con las herramientas necesarias para hacerlo.

- En ese sentido y teniendo en cuenta que al estar tan inmersos en el mundo de la internet, con los riesgos que ello implica, deba el estado crear las mejores condiciones para que los usuarios puedan acudir a su utilización convencidos que existen mecanismos preventivos y que además, en caso de que se vulneren aquellos mecanismos, se cuenten con las condiciones jurídicas necesarias para enfrentar, asumir y sancionar a quien opte por perjudicar el patrimonio de algún individuo.

- Un punto de partida de suma importancia en la consolidación de nuevos mecanismos proteccionistas en contra de ciberdelincuencia, sin duda, es el principio de legalidad, puesto que a partir de él, se debe permitir la construcción y reconocimiento de nuevos modelos delictivos para poder hacerle frente, es decir, si conocemos a que nos enfrentamos, por supuesto que sabremos de que manera podemos actuar. Este principio es base y necesario en la respuesta que provenga del estado, sin él, es posible que se incurra en situaciones de anomia normativa y por ende en impunidad.

- No se trata crear tipos penales de manera arbitraria o de modificar la ley penal en detrimento de los asociados, puesto que podría generar situaciones de inseguridad jurídica que permean al sistema judicial y lo hacen débil. Se trata de brindar las mejores herramientas a los operadores de justicia, quienes son el ultimas quienes se enfrentan a estos nuevos retos y de quienes

se espera justicia, misma, que esperan los delincuentes con la imposición de la sanción acorde con el delito cometido.

- Si ello es así, y estamos enfrentados a un nuevo ciber mundo, porque no reconocer dentro de las nuevas modalidades de delito aquellas cometidas a través de medios electrónicos, ya se dio un paso inicial como en efecto sucedió con el hurto, porque no hacerlo a través de la modificación del artículo 247 del Código Penal, al que no es posible acudir cuando la estafa es cometida a través de ellos, quedando desprovista de intervención especial, independientemente si en la comisión del hecho se utilizaron diversas herramientas tecnológicas y posibilitaron en mayor medida, debido a la manipulación, la consumación del acto.

- La razón de pedir está inclusión en los agravantes de la estafa, se centra en la degradación que sufre el delito cuando para su consumación se utilizan diversos medios electrónicos, que son de difícil o imposible detección, pero que sin importar el perjuicio patrimonial, queda desprovisto de intervención, al no poderse acudir a los agravantes de la conducta por no estar contemplados como tal.

- No es un capricho la necesidad de incluir dentro del artículo 247 el agravante de la estafa a través de medios electrónicos es una realidad social carente de protección, puesto que la sanción simple impuesta a través del tipo penal base luce menor en relación con las afectaciones que se llevan a cabo a través de las plataformas de la internet, que valga la pena mencionar no pueden concurrir ni asumirse como hurtos a través de medios informáticos por ser delitos de diferente esencia.

- Se espera, que de estas pequeñas conclusiones, puedan surgir las herramientas necesarias que posibiliten la modificación del Código Penal.

Conclusiones y recomendaciones

- El primer reto asumido con la presente investigación se basó en la necesidad de establecer de la mejor manera los marcos teóricos que nos permitieran avanzar con solides en la búsqueda de las herramientas necesarias de la demostración de la necesidad de modificar el Código Penal Colombiano, en lo referente al delito de estafa y sus agravantes. Estos elementos, fueron al inicio de la misma una labor importante, porque, además de buscar de manera local, se hacía necesario y por el contexto de la investigación, analizar algunos referentes internacionales que nos dieran pistas sobre el asunto.

- Asumido el reto, la investigación se enfoca de manera concreta en primero, estudiar desde la normativa Española, el manejo dado a los delitos cometidos por medios electrónicos, claro, y antes, como era necesario, se aporta todo un contexto global que nos permite identificar aspectos de suma importancia en el conocimiento de lo que se conoce como ciber delitos. Desde allí, se mostraron los primeros indicios en esa nueva generación de delitos y por supuesto de los nacientes delincuentes.

- Importante, fue analizar el medio en el que estos nuevos delincuentes se mueven, puesto que, en su momento, la naciente herramienta llamada internet, creo condiciones especiales que fueron identificadas rápidamente por los delincuentes, por lo que el estudio de factores también se centró en reconocer aquellos que le eran propicios para la consumación de estos nuevos delitos. El reto en este punto, (por fortuna superado) fue rastrear aquellas otras bases de datos que nos mostraran, no solo en España, cómo venía desarrollándose el delito cometido a través de medios electrónicos y por supuesto el impacto de ellos en la sociedad.

La demostración del primer objetivo estuvo sustentado en la necesidad de consolidar toda esa información y crear la bases teóricas para el desarrollo de los demás objetivos.

- Estamos convencidos que uno de los aspectos más importantes en este primero objetivo fue evidenciar el crecimiento desmedido de la internet, vista esta como una herramienta necesaria en una sociedad que cada día requiere de ella para la realización de tareas que hace algún tiempo demandaba de la presencia de la persona. Transacciones bancarias y muchas otras cosas más, aportan, o hacen mucho más fácil la vida cotidiana, a la par que brinda a los delincuentes espacios infinitos para la consumación de sus actos criminales. Y es en este punto, en donde, a fin de crear herramientas que le hagan frente a esta nueva modalidad delictiva, se empieza a hacer necesario el cambio de políticas criminales que la entiendan y que brinde a los operadores judiciales las herramientas necesarias para la defensa de la sociedad.

- El segundo paso, se centró en el estudio doctrinal y jurisprudencial de aquellos elementos que hacen parte del delito de estafa y sus agravantes. Fue necesario, desmenuzar todos aquellos componentes del tipo penal para entender si efectivamente pudiera ser viable la modificación de nuestro Código Penal en la inclusión de un nuevo agravante que reconociera la cometida a través de medios electrónicos. Paso de suma importancia si se tiene en cuenta que algunas voces han manifestado que a la postre se trata de un hurto dado el fin perseguido por los delincuentes, el cual, normalmente esta orientado al dinero. Sin embargo, el capítulo II, deja en claro y de manera acertada que se trata de estructuras diferentes, de tipos penales que a pesar de compartir el mismo bien jurídico tutelado, son independientes en los que distan mucho los mecanismos utilizados para su consumación, por lo que, independientemente de si en el hurto se utilizan medios electrónicos en él no

concurre el engaño como si en la estafa, por lo que se hace imposible su comparación y menos atribuir la conducta al artículo 239 cuando en realidad nos referimos a la estafa.

- Por ello y a pesar de ser bastante extenso en segundo capítulo, brinda herramientas importantes en la comprensión de este delito, aporte necesario en el estudio del derecho penal y por supuesto de la parte especial de nuestro Código Penal, por ende, más que extenso, es, en todo, robusto en su demostración y determinación de los elementos estructurantes de la modificación pretendida y de forzoso estudio de cara al capítulo III en el que se expusieron y demostraron los pormenores de la inevitable modificación del artículo 247 sustantivo penal Colombiano.

- Aspecto importante en la construcción del capítulo III, fue hacer un estudio de uno de los elementos más significativos del Derecho Penal, como lo es el principio de legalidad, sobre el cual se ha sustentado en mucho su historia y el cual es punto de partida en esta materia, puesto que sin él, es muy posible que se incurran en arbitrariedades no solo para las víctimas sino para quienes esperan ser juzgados de acuerdo a las normas y leyes previamente reconocidas en el ordenamiento jurídico nacional. Así las cosas, se requería en esta investigación, dejar sentadas la bases en cuanto a exigencia de que en materia penal prima la aplicación de la ley vigente al momento y la prohibición expresa de analogía para resolver casos que no estén contemplados como delitos.

- Este inicio es, sin duda alguna, uno de los elementos de mayor importancia en la demostración de la necesidad de modificar el artículo 247 del Código Penal y reconocer como agravante la estafa cometida a través de medios informáticos, puesto que, como lo señala la misma legislación no es posible imponer una sanción penal por un hecho no

reconocido como penable. Luego, en aras de las garantías constitucionales, se mostró el camino que debe seguirse en cuanto al imperativo legal y por supuesto Constitucional. Claro, el estudio en este punto no solo requería analizar al principio de legalidad, sino además, establecer de qué manera su no reconocimiento podría impactar en la determinación de responsables por hechos en los que concurran estos factores. Por fortuna, para la investigación, y amparados en él, se pudo concluir que en materia penal se hace indispensable una modificación que entienda esta nueva modalidad de delito para así poder sancionar de manera efectiva a quien asume como posible este camino.

- El riesgo en la actualidad, surge de la inexistencia normativa, de la anomia, que se convierte en el primer enemigo en la lucha contra la delincuencia. Delincuencia que día a día se profesionaliza y que en encuentra en estos vacíos los escenarios propicios para la consumación de sus actos y que a la postre pueden generar impunidad, puesto que lo que se espera es que la sanción no quede disminuida o reducida ante la inexistencia legal. Es claro, que a la fecha se castiga la estafa, pero, existen referentes normativos penales, en los que si se tomo la decisión de reconocer estas nuevas facetas delictivas, somo sucede con el artículo 269I, el cual, de acuerdo a unas condiciones remite la aplicación de la ley al artículo 239 del Código Penal.

- Si ello es así, es porque se entienden los diferentes medios que pueden llegar a influir en la comisión de este tipo de delitos y su reconocimiento en el ordenamiento legal busca el brindar las mejores garantías a las partes del proceso, independientemente la condición en la que se presenten. Esta es una necesidad basada en la Constitución y en la misma evolución del derecho penal que exige como principio fundamental la legalidad.

- Al revisar los elementos anteriores, se llegó a la evidente conclusión que es imperativo, necesario y casi que obligatorio, modificar el Código Penal en su artículo 237 e incluir el agravante cuando la estafa se comete a través de medios electrónicos, puesto que nuestro proceso penal exige y debe promulgar no solo el respecto a las partes, sino como fin esencial del estado garantizar el cumplimiento de las normas de índole constitucional para su consagración.

- El impacto de la presente investigación radica no solo en el valioso aporte académico, en el cual se muestran todos y cada uno de los factores que confluyen en la comisión del delito de estafa, surgiendo como una herramienta de estudio en el esclarecimiento de dudas frente a los delitos de hurto cometido a través de medios electrónicos y éste, además de mostrarnos un camino claro en el que se trazan los lineamientos de lo que debería ser una forma inmediata de la legislación penal.

- La sociedad espera del estado una mayor intervención y control en la evitación de este tipo de delitos, pero, una vez consumados, esperan de la administración de justicia una actividad acorde con el crimen cometido, por lo que, sería de suma importancia poder llevar el presente documento a diversos entes estatales, incluyendo Congreso de la República, en búsqueda de su estudio profundo y por supuesto, porque no, lograr a futuro la imperiosa modificación aquí demostrada, en aras de dar cumplimiento no a la investigación sino a los imperativos legales y constitucionales analizados.

Lista de Referencias

Abushihab, M. (2016). Hurto por medios informáticos ¿un delito informático?. [Tesis de grado, Universidad Santo Tomás]. Repositorio Institucional. https://repository.usta.edu.co/handle/11634/9259.

Acurio, S. (2016). Delitos informáticos: Generalidades. (ed.) Dspace. https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf.

Arteaga, A. (1975). *La culpabilidad en la teoría del hecho punible*. Editorial Universidad Central de Venezuela.

Barrios, S. (2012). El delito informático en la legislación Colombiana. [Tesis de grado, Corporación Universitaria de la Costa C.U.C.]. Repositorio Institucional. https://repositorio.cuc.edu.co/bitstream/handle/11323/905/EL_DELITO_INFORMATICO_EN_LA_LEGISLACION_INFORMATICA.pdf?sequence=1&isAllowed=y.

Beccaria, C. (2015). Tratado de los delitos y de las penas. Manuel Martínez Neira. Universidad Carlos III de Madrid. https://e-archivo.uc3m.es/bitstream/handle/10016/20199/tratado_beccaria_hd32_2015.pdf

Beltrán, A. y Carrillo, J. (2017). El acceso abusivo a sistemas informáticos en el ordenamiento jurídico Colombiano: Problemáticas y propuesta para su superación. [Tesis de grado, Universidad del Rosario]. Repositorio Institucional. https://repository.urosario.edu.co/handle/10336/13979.

Bustamante, L. (1979). *El patrimonio. Dogmática jurídica*. Editorial Jurídica de Chile.

Bustos, M. y Torres. G, (2018). Concepción de los delitos informáticos en Colombia y la legislación actual. [Tesis de grado, Universidad de Santiago de Cali]. Repositorio Institucional. https://repository.usc.edu.co/handle/20.500.12421/1567?show=full.

Cano, A., Díaz. J., Mendieta, C., Rivas, C. y Sánchez, N. (2014). Aporte internacional frente a los delitos informáticos en Colombia y su ejecución por parte de las autoridades competentes. [Tesis de grado, Universidad Libre de Colombia]. Repositorio Institucional. https://repository.unilibre.edu.co/handle/10901/7695.

Casado, I. (2017). Estafas cometidas a través de compras online. [Tesis de grado, Universidad del País Vasco]. Repositorio Institucional. https://addi.ehu.es/bitstream/handle/10810/29866/Irene%20Casado%20Perez.pdf?sequence=1&isAllowed=y.

Condori, M. (2013). Phishing. *Revista de información, tecnología y sociedad*, *8*(2), 34-35. http://www.revistasbolivianas.org.bo/scielo.php?script=sci_arttext&pid=S1997-40442013000100015&lng=en&nrm=iso.

Constitución política de Colombia [Const. P.] (1991). Colombia. Obtenido el 21 de febrero de 2021. http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991_pr003.html#115

Convenio. (2001). Convenio sobre la Ciberdelincuencia. Consejo de Europa. Obtenido el 14 de septiembre de 2022. http://chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Corte Constitucional [C.C.], enero 22, 2004, M.P: M. Cepeda. Sentencia T-025/04. Colombia. 10/02/2020. https://www.corteconstitucional.gov.co/relatoria/2004/t-025-04.htm

Corte Constitucional [C.C.], enero 23, 2008, M.P: R. Escobar. Sentencia C-030/08. Colombia. 10/02/2020. https://www.corteconstitucional.gov.co/relatoria/2008/c-030-08.htm

Corte Suprema de Justicia [C.S.J], junio, 2006, M.P: M. Solarte. Sentencia. Obtenido el 9 de junio de 2021. Colombia. file:///C:/Users/24-r101la/Downloads/format%20(14).html

Corte Suprema de Justicia [C.S.J], junio, 2003, M.P: A. Pérez. Sentencia 17196. Obtenido el 9 de junio de 2021. Colombia. file:///C:/Users/24-r101la/Downloads/format%20(14).html

Decreto 2374/93, noviembre 30, 1993. Ministerio de Educación Nacional. (Colombia). Obtenido en 10 de febrero de 2020. https://www.mineducacion.gov.co/1621/articles-104283_archivo_pdf.pdf

Decreto 2613/13, noviembre 20, 2013. Ministerio del Interior. (Colombia). Obtenido el 10 de febrero de 2020. https://www.mininterior.gov.co/sites/default/files/11_decreto_2613_de_2013.pdf

Díaz, A. (2009). http://legalidadinformatica.blogspot.com/2009/12/tratamiento-y-delitos-de-violacion-de.html.

Díez, P. (1979). *La Estafa*. Editorial Tirant Lo Blanch.

Evans, D. (2011). Internet de las cosas. Cómo la próxima evolución de internet lo cambia todo. *Revista Cisco IBSG*. https://www.cisco.com/c/dam/global/es_mx/solutions/executive/assets/pdf/internet-of-things-iot-ibsg.pdf.

Feuerbach, P. (2010). J.A. Anti-Hobbes. O Sobre los límites del poder del poder supremo y el derecho de coacción del ciudadano contra el soberano, Hammurabi, Buenos Aires. http://www.derecho.uba.ar/publicaciones/lye/revistas/91/comentario-bibliografico-de-anti-hobbes-o-sobre-los-limites-del-poder-supremo-y-el-derecho-de-coaccion-del-ciudadano-contra-el-soberano.pdf

García, N. (2005). *Estructura jurisprudencial del delito de estafa*. Editorial Iustel Madrid.

Gerencia de Innovación y Desarrollo Tecnológico – GIDT. (2013). Phishing. https://gidt.unad.edu.co/gidt/seguridad-de-la-informacion/noticias-seguridad/76-phishing1.

Giraldo, J. y Duarte. I. (2018). Ingeniería Social: Técnica de ataque Phishing y su impacto en las empresas Colombianas. [Tesis de grado, Universidad Nacional Abierta y a Distancia UNAD]. Repositorio Institucional. https://repository.unad.edu.co/bitstream/handle/10596/27050/jpgiraldoma.pdf?sequence=1&isAllowed=y.

García, D. (2017).El Phishing como delito de estafa informática. Comentario a la SAP de Valencia 27/2017 de 25 de enero (Rec. 1402/2016). *Revista. Boliv. De Derecho, 25*, 650-659. https://dialnet.unirioja.es/servlet/articulo?codigo=6263417.

Gómez, R., Rey, B., Villarreal, R., Puello, R., Amador, C., Montoya, G., Ballesteros, E., Hernández, H. y Camacho, J. (2015). Configuraciones del Derecho Penal en Colombia. (ed.) Universidad Libre de Colombia. http://www.unilibre.edu.co/cartagena/pdf/investigacion/libros/derecho/CONFIGURACIONES_DEL_DERECHO_PENAL_EN_COLOMBIA.pdf.

Grosso, M. (2019). Principio de legalidad. Un estudio semiótico de su génesis, destrucción y construcción en el contexto del Derecho Penal. Editorial Euros Editores S.R.L.

Hernández, H. (2010). Normativización del engaño y nivel de protección de la víctima en la estafa: lo que dice y no dice la dogmática. *Revista Chilena de Derecho, 37*-1. https://www.scielo.cl/scielo.php?script=sci_nlinks&ref=6470404&pid=S0718-34372014000300010000071&lng=es.

García, D. (2017).El Phishing como delito de estafa informática. Comentario a la SAP de Valencia 27/2017 de 25 de enero (Rec. 1402/2016). *Revista. Boliv. De Derecho, 25*, 650-659. https://dialnet.unirioja.es/servlet/articulo?codigo=6263417.

Ley 70/93, agosto 27, 1993. Diario Oficial. [D.O.]: 41.013. (Colombia). Obtenido el 10 de febrero de 2020. https://www.acnur.org/fileadmin/Documentos/BDL/2006/4404.pdf?file=fileadmin/Documentos/BDL/2006/4404

Ley 89/90, noviembre 25, 1890. Ministerio de Interior. [OIPI]. (Colombia). Obtenido el 10 de febrero de 2020. https://www.mininterior.gov.co/la-institucion/normatividad/ley-89-de-1890

Leyton, J (2014). Los elementos típicos del delito de estafa en la doctrina y jurisprudencia comtemporáneas. *Revista ARS Boni Et Aequi, 10*(2), 123-161. http://www.ubo.cl/icsyc/wp-content/uploads/2014/12/123-161.pdf.

López, J. y Sáenz, M. (2018). La obtención de la prueba penal internacional en materia de delitos cibernéticos. [Tesis de grado, Universidad Politécnico Gran Colombiano]. Repositorio Institucional.

https://alejandria.poligran.edu.co/bitstream/handle/10823/1501/Ciberdelitos%20%28Monica%20Saenz%20-%20Jessica%20Lopez%29-Ultima%20version%20corregida.pdf?sequence=1&isAllowed=y.

Mayer, L. (2014). El engaño concluyente en el delito de estafa. *Revista Chilena de Derecho, 41*(3), 1017-1048. https://scielo.conicyt.cl/scielo.php?script=sci_abstract&pid=S0718-34372014000300010&lng=es&nrm=iso.

Mesa, L. (1979). *Lecciones de derecho penal*. Universidad Externado de Colombia.

Montañez, A. (2017). Análisis de los delitos informáticos en el actual sistema Penal Colombiano. [Tesis de grado, Universidad Libre de Colombia]. Repositorio Institucional. https://repository.unilibre.edu.co/bitstream/handle/10901/11041/AN%C3%81LISIS%20DE%20LOS%20DELITOS%20INFORM%C3%81TICOS%20EN%20EL%20ACTUAL%20SISTEMA%20PENAL%20COLOMBIANO%20revisado%20NHJ%20OK.pdf?sequence=3&isAllowed=y.

Morales, J. (2020). https://www.eltiempo.com/tecnosfera/novedades-tecnologia/estafas-en-internet-han-aumentado-durante-la-pandemia-del-coronavirus-486284.

Mosquera, V. (2019). Ciberseguridad en Colombia. *Revista Universidad Piloto de Colombia,* 1-6. http://polux.unipiloto.edu.co:8080/00001886.pdf

Muñoz, F. (1995). *Derecho Penal, parte especial*. Editorial Tirant lo Blanch.

Naciones Unidas Derechos humanos. (diciembre, 1965). Convención Internacional sobre la Eliminación de todas las Formas de Discriminación Racial. Trabajo presentado en la

Asamblea General en su resolución 2106 A (XX). Colombia. https://www.ohchr.org/Documents/ProfessionalInterest/cerd_SP.pdf

Narváez, D. (2015). El delito informático y su clasificación. *Revista de ciencia, Tecnología e Innovación*, *2*(2), 158-173. http://45.238.216.13/ojs/index.php/EPISTEME/article/view/102.

Narváez, G. (2014). https://es.slideshare.net/gambitguille/enfoques-de-investigacion-37890633.

Oficina de las Naciones Unidas contra la Droga el Delito UNODC. (2013). *Manual sobre los delitos relacionados con la identidad*. Naciones Unidas.

Ojeda, J., Arias, M., Rincón, F. y Daza L. (2010). Delitos informáticos y entorno jurídico vigente en Colombia. *Revista Cuad. Contab./Bogotá*, *11*(28), 41-66. http://www.scielo.org.co/scielo.php?pid=S0123-14722010000200003&script=sci_abstract&tlng=es.

Oxman, N. (2013). Estafas informáticas a través de Internet: acerca de la imputación penal del "phishing" y el "pharming"**.** *Revista de Derecho de la Pontificia Universidad Católica de Valparaiso*, *41*(2), 211-262. https://www.scielo.cl/pdf/rdpucv/n41/a07.pdf.

Pabón, P. (2013). *Manual de derecho penal: parte especial*. Ediciones Doctrina y Ley Ltda.

Pabón, P. (2013). *Manual de derecho penal: parte general*. Ediciones Doctrina y Ley Ltda.

Pastor, N. (2004). *La determinación del engaño típico en el delito de estafa*. Editorial Marcial Pons.

Quevedo, J (2017). *Investigación y prueba del ciberdelito*. [Tesis Doctoral, Universitat de Barcelona].

https://www.tdx.cat/bitstream/handle/10803/665611/JQG_TESIS.pdf?sequence=1&isAllowed=y.

Riascos, L (2012). Los delitos contra los datos personales y el habeas data en la Ley 1273 de 2009. *Derecho y Realidad*, *20*(2), 335-429. https://revistas.uptc.edu.co/index.php/derecho_realidad/article/view/4868.

Rico, M. (2012). Los desafíos del derecho penal frente a los delitos informáticos y otras conductas fraudulentas en los medios de pago electrónicos. *Revista del Instituto de Ciencias Jurídicas de Puebla, México, 7*(31), 207-222. http:///C:/Users/24-r101la/Downloads/Dialnet-LosDesafiosDelDerechoPenalFrenteALosDelitosInforma-4646214.pdf.

Sotomayor, J. (2007). Las recientes reformas penales en Colombia: un ejemplo de irracionalidad legislativa. *Nuevo Foro Penal*, *71*, 13-66. https://dialnet.unirioja.es/servlet/articulo?codigo=3823011.

Suárez, A. (2013). *Delitos contra el patrimonio económico*. Editorial Universidad Externado de Colombia.

Welivesecurity en su publicación realizada para el 12 de noviembre del año 2013. https://www.welivesecurity.com/la-es/2013/12/02/resumen-amenazas-noviembre-2013/.