



UNIVERSIDAD NACIONAL DE LOJA

Área Jurídica Social y Administrativa

CARRERA DE DERECHO

**La Falta de Tipificación del Delito de
Estafa informática en el Código Orgánico
Integral Penal (COIP), perjudica el
Patrimonio de las personas.**

TESIS PREVIA A OPTAR POR EL
GRADO DE LICENCIADA EN
JURISPRUDENCIA Y TÍTULO DE
ABOGADA

AUTORA:

Claudia Karina Medina González

DIRECTOR:

Dr. José Dositeo Loaiza Moreno

LOJA-ECUADOR
2021

II. CERTIFICACION

Doctor

José Dositeo Loaiza Moreno

**DOCENTE DE LA CARRERA DE DERECHO DE LA UNIVERSIDAD
NACIONAL DE LOJA**

CERTIFICO:

Que la tesis titulada “**La Falta de Tipificación del Delito de Estafa Informática en el Código Orgánico Integral Penal (COIP), perjudica el Patrimonio de las personas.**” Realizado por la señorita estudiante Claudia Karina Medina González, previo a la obtención de grado de licenciada en Jurisprudencia, ha sido cuidadosamente revisada por lo que he podido constatar que cumple con todos los requisitos de fondo y de forma establecidos para esta clase de trabajos, por lo que autorizo su presentación y disertación.

Loja, 27 de Julio del año 2020



Firmado electrónicamente por:
**JOSE DOSITEO
LOAIZA MORENO**

Dr. José Dositeo Loaiza Moreno
DIRECTOR DE TESIS

III. DECLARACIÓN DE AUDITORIA

Yo, Claudia Karina Medina González, declaro que el presente trabajo de tesis es original y de mi autoría, que se ha citado las fuentes correspondientes y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos o acciones legales, por el contenido de la misma.

Adicionalmente acepto y autorizo a la Universidad Nacional de Loja, la publicación de mi tesis en el Repositorio Institucional – Biblioteca Virtual.



Verificado digitalmente por:
CLAUDIA KARINA
MEDINA GONZALEZ

AUTORA: Claudia Karina Medina González

C.I: 1900663970

Loja, 02 de marzo del 2021

IV. CARTA DE AUTORIZACIÓN DE TESIS POR PARTE DEL AUTOR, PARA LA CONSULTA, REPRODUCCIÓN PARCIAL O TOTAL Y PUBLICACIÓN ELECTRONICA DEL TEXTO COMPLETO

Yo, Claudia Karina Medina González declaro ser autora de la tesis titulada “**LA FALTA DE TIPIFICACIÓN DEL DELITO DE ESTAFA INFORMÁTICA EN EL CÓDIGO ORGÁNICO INTEGRAL PENAL (COIP), PERJUDICA EL PATRIMONIO DE LAS PERSONAS**”. Como requisito para optar al grado de: **Licenciada en Jurisprudencia y Título de Abogada**, autorizo al Sistema Bibliotecario de la Universidad de Loja para que, con fines académicos, muestre al mundo la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Digital Institucional:

Los usuarios pueden consultar el contenido de este trabajo en el RDI, en las redes de información del país y del exterior, con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja no se responsabiliza por el plagio o copia de tesis que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los dos días del mes de marzo del dos mil veintiuno, firma el autor.

Autora: Claudia Karina Medina González

C.I.: 1900663970

Dirección: Loja, Sucre entre Quito y José Félix Valdivieso

Correo electrónico: kerina1210@gmail.com, ckmedinag@unl.edu.ec

Teléfono Celular: 0994438821

DATOS COMPLEMENTARIOS

Director de Tesis: Dr. José Dositeo Loaiza Moreno

Tribunal de Grado

Presidente: Dr. Shandry Vinicio Armijos Fierro, Mg.Sc

Vocal: Dr. Fernando Filemón Soto Soto, Mg.Sc

Vocal: Dr. Ángel Medardo Hoyos Escaleras, Mg.Sc

IV.DEDICATORIA

El presente trabajo va dedicado a mis padres, hermanos y familia, por haberme guiado, brindado su apoyo incondicional, sacrificio y confianza, para poder realizar y culminar mis estudios. A mi hija Erika la razón y el motivo de querer superarme día a día, por su paciencia y cariño.

Claudia Medina

V. AGRADECIMIENTO

A Dios, por la vida porque me ha permitido cumplir metas, continuar con mis sueños y aventuras. A la Universidad Nacional de Loja, a su Área Jurídica Social y Administrativa de manera especial a la Carrera de Derecho por acogerme, prepararme y educarme en sus aulas durante toda mi carrera universitaria.

A los docentes por haberme transmitido sus valiosos conocimientos, experiencias y apoyo académico. De manera especial al Doctor Mario Sánchez, como docente de Titulación, me guío a cada paso de la elaboración del proyecto y de la presente tesis, a mi Director de tesis, por convertirse en mi mentor y abrirme las puertas de su conocimiento en cada paso dado en este camino de titulación.

A mi familia por brindarme su apoyo, ayudarme cuando más los necesite, mis padres y hermanos por el cariño brindado hacia mí y mi hija, permitiéndome con su constante apoyo continuar con mis estudios.

Finalmente, a mis amigos y compañeros de la Facultad de Derecho por darme una mano en momentos difíciles, por todo lo compartido durante nuestra formación académica y el ánimo mutuo a seguir para llegar a ser parte del grupo de los profesionales del Derecho, objetivo común que nos hemos planteado.

LA AUTORA

VI. TABLA DE CONTENIDOS

I.	PORTADA	
II.	CERTIFICACION	
III.	DECLARATORIA DE AUDITORIA	
IV.	CARTA DE AUTORIZACIÓN	
V.	DEDICATORIA	
VI.	TABLA DE CONTENIDOS	

1.	TITULO	1
2.	RESUMEN	2
2.1.	ABSTRACT	5
3.	INTRODUCCIÓN	8
4.	REVISION DE LITERATURA	11
4.1.	Marco Conceptual	11
4.1.1.	Tipo	11
4.1.2.	Tipicidad	12
4.1.3.	Delito	13
4.1.4.	Patrimonio	16
4.1.5.	Violación a la Privacidad de Datos	17
4.1.6.	Estafa	19
4.1.7.	Tecnologías de la Información y la Comunicación	20
4.1.8.	Estafa Informática	24
4.2.	Marco Doctrinario	25
4.2.1.	Las Tecnologías de la información y la Comunicación Tics en un mundo globalizado	25
4.2.2.	Avances de la Tecnologías de la Información y la Comunicación	28
4.2.3.	Tipos de Tecnologías de la Información y la Comunicación	31

4.2.4. Elementos que configuran el delito de Estafa Común	35
4.2.5. Delitos Informáticos	37
4.2.6 Elementos para que se configure el delito de estafa informática.....	46
4.2.7 Diferencias entre estafa y estafa informática.....	59
4.3. MARCO JURÍDICO.....	62
4.3.1. La Protección al Derecho a la Propiedad en la Constitución de la República del Ecuador.....	62
4.3.2. Estafa Informática en Leyes y tratados Internacionales	63
4.3.3. El Delito de Estafa en Código Orgánico Integral Penal (COIP).....	65
4.3.4 De la extraterritorialidad de los delitos.....	74
4.3.5 Tipificación del delito de Estafa Informática en el Derecho Comparado..	75
5. MATERIALES, TÉCNICAS Y METODOS	77
5.1. Materiales.....	77
5.1.1. Materiales de Oficina.....	77
5.1.2. Materiales bibliográficos	77
5.2. Técnicas.....	78
5.2.1. La Encuesta.....	78
5.2.2. La Entrevista	79
5.3. Métodos	79
5.3.1. Método Inductivo	79
5.3.2. Método Deductivo	80
5.3.3. Método Analítico	80
5.3.4. Método Comparativo	80
6. Resultados de la Investigación de Campo	81
6.1. Resultados de las Encuestas	81
6.2 Resultados de las Entrevistas	90
7. Discusión	106
7.2. Verificación de Objetivos	106
7.2.1. Objetivo General.....	107
7.2.2. Objetivos Específicos.	108
7.3. Contrastación de la Hipótesis.....	109
7.4. Fundamentación Jurídica para la Propuesta de Reforma Legal.....	110

8. Conclusiones.	112
9. Recomendaciones	113
10. Propuesta Jurídica	114
11. Bibliografía	119
12. Anexos	125
12.1. Proyecto de Tesis	125
12.2. Encuesta	161
12.3. Entrevista	163

1. TITULO

La Falta de Tipificación del Delito de Estafa Informática en el Código Orgánico Integral Penal (COIP), perjudica el Patrimonio de las Personas.

2. RESUMEN

Los avances de la tecnología de la información y la comunicación, evolucionan día tras día prestando facilidades en varios aspectos de la vida y en el desenvolvimiento de la Sociedad, pero al mismo tiempo consigo han arrastrado ciertas desventajas por poseer la característica de libre acceso, dando lugar a un surgimiento de nuevas formas de delinquir o a su vez una evolución de las formas de cometer actividades ilícitas; por el sin número de información personal que el usuario ingresa, en la variedad de aplicaciones que la tecnología ofrece, como las populares redes sociales o las compras en línea. Éstas conductas de las que hablo en el presente trabajo de investigación como objeto de esta investigación considerando que son las siguientes: La inserción de enlaces (links) fraudulentos en redes sociales y correos electrónicos para la obtención de información personal y confidencial, ofertas de trabajo u actualización de datos (Phishing), la inserción de enlaces o mensajes fraudulentos a través de la telefonía móvil para obtener información personal y confidencial, una forma común son las promesas de haber ganado un premio de cuantioso valor (Smishing); y, por último el uso de llamadas programadas de forma simultáneas a diferentes números, mediante el cual obliga al usuario a llamar al número asignado so pena de ver perjudicado su patrimonio en su cuenta bancaria (Vishing), conductas que doctrinariamente y en otras legislaciones las conocen o tipifican como estafa informática.

Nuestro país tipifica en el Artículo 186 del vigente Código Orgánico Integral Penal acciones similares a las conductas antes mencionadas en su numeral 2, referentes a la estafa común, a la defraudación en dispositivos de uso bancario específicamente “cajero bancario”, perjuicio o engaño al consumidor entre otros, lo que provoca que

la Fiscalía General del Estado, adecue otras modalidades de estafa informática en este tipo penal de estafa común.

A lo largo del desarrollo de la presente investigación abordaré y desarrollaré temas que permitirán realizar una diferenciación entre el delito de estafa común y estafa informática, la importancia que se encuentre tipificada de manera independiente en nuestro Código Orgánico Integral Penal, la estafa informática; considerando que es un producto de los avances de las tecnologías de la información y la comunicación, enfocado en producir una afectación al patrimonio de las personas.

El presente trabajo se desarrolla inicialmente con una breve reseña histórica de la evolución de las tecnologías desde su descubrimiento, sus tipos y usos que se le da a cada uno, hasta llegar a determinar los elementos que deben estar presentes para que se configure el delito de estafa común y estafa informática apoyados en un estudio y descripción de cada una de las modalidades de estafa informática tema principal de la presente investigación, así como una diferenciación entre ambos delitos.

Sin dejar de lado el análisis de nuestra legislación constitucional para identificar el bien protegido al que afecta el delito de estafa informática, y en cómo se relaciona con la seguridad jurídica, el principio de legalidad y a la interpretación literal de la ley, estipulados en su Artículo 13 y 5, inciso 1, respectivamente articulado perteneciente al Código Orgánico Integral Penal. Sin dejar de lado los recursos normativos internacionales que otorga el Derecho, cuyo valor es muy elevado en la presente investigación por su aporte referencial como el Convenio sobre Ciberdelincuencia celebrado en Budapest para los países europeos y fuente de guía

para legislaciones de países que si tienen tipificado el delito de estafa informática de una manera más autónoma e independiente a el delito de estafa común.

Concluyo con el planteamiento de una propuesta jurídica de reforma acorde a la realidad actual, social y tecnológica, basada en razones y fundamentos extraídos del estudio jurídico, con respeto a los mandatos constitucionales siendo el principio de legalidad, uno de los principios fundamentales para poder sancionar a una persona, y la interpretación literal de la norma. Con ello, no se deja en tela de duda la necesidad de implementar dentro del catálogo de delitos informáticos a la figura de estafa informática y sus modalidades, para de esta forma garantizar la protección del patrimonio y propiedad de las personas.

2.1. ABSTRACT

The advances in information and communication technology evolve day after day, providing facilities in various aspects of life and in the development of the Society, but at the same time they have brought certain disadvantages due to having the characteristic of free access, giving lead to the emergence of new forms of crime or in turn an evolution of the forms of committing illicit activities; due to the number of personal information that the user enters, in the variety of applications that technology offers, such as popular social networks or online purchases. These behaviors that I speak of in this research work as the object of this research considering that they are the following: The insertion of fraudulent links in social networks and emails to obtain personal and confidential information, job offers or data updating (Phishing), the insertion of fraudulent links or messages through mobile telephony to obtain personal and confidential information, a common form is the promises of having won a prize of considerable value (Smishing); and, finally, the use of calls programmed simultaneously to different numbers, by means of which the user is obliged to call the assigned number under penalty of seeing his assets in his bank account harmed (Vishing), behaviors that doctrinally and in other laws known or typified as a computer scam.

Our country typifies in Article 186 of the current Comprehensive Organic Criminal Code actions similar to the behaviors mentioned above in its numeral 2, referring to the common fraud, fraud in devices for banking use specifically "bank teller", damage or deception to the consumer among others, which causes the State Attorney General's Office to adapt other forms of computer fraud in this criminal type of common fraud.

Throughout the development of this research, I will address and develop issues that will allow a differentiation between the crime of common fraud and computer fraud, the importance that is classified independently in our Comprehensive Organic Criminal Code, computer fraud; considering that it is a product of the advances of information and communication technologies, focused on producing an impact on people's assets.

This work is initially developed with a brief historical review of the evolution of technologies from their discovery, their types and uses that are given to each one, until determining the elements that must be present for the crime of common scam and computer scam supported by a study and description of each of the types of computer scam main topic of this research, as well as a differentiation between both crimes.

Without neglecting the analysis of our constitutional legislation to identify the protected asset that is affected by the crime of computer fraud, and how it relates to legal security, the principle of legality and the literal interpretation of the law, stipulated in its Article 13 and 5, subsection 1, respectively articulated pertaining to the Comprehensive Organic Criminal Code. Without leaving aside the international normative resources granted by the Law, whose value is very high in the present investigation due to its referential contribution such as the Convention on Cybercrime celebrated in Budapest for European countries and a source of guidance for legislation of countries that do have criminalization the crime of computer fraud in a more autonomous and independent way than the crime of common fraud.

I conclude with the presentation of a legal reform proposal according to the current social and technological reality, based on reasons and foundations extracted from the legal study, with respect to the constitutional mandates, being the principle of legality, one of the fundamental principles to be able to sanction to a person, and the literal interpretation of the rule. With this, the need to implement the figure of computer fraud and its modalities within the catalog of computer crimes is not questioned, in order to guarantee the protection of people's assets and property.

3. INTRODUCCIÓN

La presente investigación se encuentra enfocada en las nuevas formas de delinquir que han surgido como consecuencia de los avances de las tecnologías de la información y la comunicación, parte del mundo globalizado y tecnológico en el que vivimos hoy en día, que se constituyen en mecanismos de: inserción de enlaces fraudulentos en redes sociales y correos electrónicos con la única finalidad de la obtención de información personal y confidencial, propia o de terceras personas. La forma más común de propagación de estos enlaces mencionados, son por medio de falsas propuestas de ofertas de trabajo u actualización de datos (Phishing), otra modalidad conocida es la ubicación de enlaces o a su vez mensajes fraudulentos por medio de la telefonía móvil ya sea a través de mensajes de texto o mediante la aplicación WhatsApp para obtener así de igual manera información personal y confidencial propia o de terceros, un texto común en dichos mensaje se constituyen de comunicados por haber ganado ciertos premios de cuantioso valor (Smishing); y, por último dentro de estas nuevas modalidades de actividades ilícitas informáticas; se encuentra el uso de llamadas programadas de forma simultáneas a diferentes números, mediante el cual obliga al usuario a llamar al número asignado so pena de ver perjudicado su patrimonio en su cuenta bancaria, va dirigida a usuarios de tarjetas de crédito ya que la forma más común es inducir al titular que sus tarjetas han sido sobrecargadas (Vishing).

Cuando una de estas conductas es ejecutada, en el plano jurídico son adecuadas al Artículo 186 del Código Orgánico Integral Penal, la estafa común, o a su vez a otros tipos penales, radicando aquí un problema en el aspecto jurídico, dado que estas adecuaciones son realizadas sin tomar en consideración que los elementos de la

estafa común no se subsumen a las conductas antes descritas, de ahí la necesidad de tipificar estas conductas como estafa informática dentro del catálogo de delitos informáticos, en consideración de la afectación significativa que provoca al patrimonio y propiedad de las personas víctimas de estas acciones.

La metodología del presente trabajo de investigación fue representada cualitativamente, especialmente por los métodos: inductivo, deductivo, analítico y comparativo; para lo cual recurrí a bibliografía necesaria a su recolección y acopio de información, que me permitieron fundamentar y posteriormente sustentarla de manera fehaciente, conceptual, doctrinaria y jurídicamente. Para obtener la investigación planteada aplique los tres objetivos específicos definidos para el desarrollo de la investigación.

El estudio teórico, normativo y doctrinario del delito de estafa informática me permitió contrastar las formas o modalidades de la misma; producto de los avances de Tecnologías de la Información y la Comunicación; en otras legislaciones, éstas conductas ya se encuentran tipificadas y sancionadas de manera autónoma, en cuerpos normativos penales, mientras que en la nuestra no se encuentra tipificada y debido a su ausencia, como lo he mencionado; son acciones adecuadas a otro tipo penal que no cumplen los parámetros y características de la conducta delictiva descrita.

El segundo objetivo planteado para esta investigación es el medio para realizar una diferenciación entre el delito de estafa común y estafa informática, aspectos de importante valor en el tema propuesto a abordar y determinando de esta forma que ciertas conductas no pueden ser sancionadas como estafa común o como otro delito

que tengan similares elementos. Con el planteamiento de la metodología adecuada me he conducido al planteamiento de interrogantes en un modelo de encuesta y entrevista dirigida profesionales el Derecho de libre ejercicio con especial enfoque para abogados especializados en Derecho Penal, los mismos que me facilitaron conocimientos y opiniones, con la finalidad de analizar la validez de mi investigación y de esta forma respaldar el tema objeto en la presente investigación.

Y por último, esta investigación busca aportar con una propuesta de reforma al Código Orgánico Integral Penal (COIP), para subsanar la ausencia que actualmente tiene, incorporando como delito autónomo a la estafa informática y sus modalidades, con elementos propios de la conducta y de esta forma, no sea confundida con otro tipo penal, con el que se daría cumplimiento al principio de legalidad establecido en el Código Orgánico Integral Penal, Artículo 5, numeral 2, así como al Artículo 13, referente a la interpretación literal de la ley, es decir, no se puede subsumir a otro tipo penal. De la misma manera esta modificación a la normativa penal protege y previene el daño patrimonial de las personas.

4. REVISION DE LITERATURA

4.1. Marco Conceptual

El presente marco conceptual se desarrolla con la finalidad de esclarecer conceptos básicos y de suma importancia, por constituirse las bases a tratar a lo largo de la investigación.

4.1.1. Tipo

Dentro de esta investigación es necesario iniciar conceptualizando el tipo por su relevancia en el ámbito de la materia penal y su relación con el problema planteado a tratar. En la doctrina encontramos que tipo es “El resultado de una reflexión del legislador sobre si una conducta debe ser sancionada en general. Pero esto son decisiones político- criminales del legislador de naturaleza pre codificadora” (Márquez Piñero, 1986, pág. 149). Con las palabras citadas puedo reflexionar que el tipo es la forma en la que se pueden plasmar soluciones sociales a los conflictos, ya que se busca con el tipo, describir específicamente a las acciones u omisiones que se deben considerar como delito y por ende la asignación de su pena correspondiente. Con esto, puedo decir que la norma penal se compone de tipo y pena.

Acertadamente se expresa que “El tipo está bajo el leitmotiv de la determinación legal, al que frecuentemente se ha reducido únicamente la legitimación de la dogmática: los tipos sirven realmente a la realización del principio nullum crimen y de él debe derivarse la estructuración dogmática” (Roxin C. 2002 pág. 58).

La tarea de tipificar delitos se encuentra dentro de las obligaciones del Estado, para dar cumplimiento con el principio de legalidad y así, enmarcar en los cuerpos legales todo lo que está prohibido y las conductas permitidas, de este modo, pretende que

para ser sujeto de una coerción debe estar dicha acción prohibitiva tipificada o descrita con precisión. En los Estados de Derecho la tarea de tipificar los delitos es únicamente del poder legislativo.

4.1.2. Tipicidad

Considero necesario continuar esta conceptualización base, tratando a la tipicidad por su aspecto fundamental en la continuación del desarrollo de la presente investigación; tanto el tipo como la tipicidad pretenden enfocarse en enmarcar toda acción u omisión que pone en peligro un bien jurídico protegido, en doctrina habla de este tema la conocida teoría de Beling. Esta teoría presenta dos corrientes pertenecientes a la teoría del delito: el causalismo y el finalismo.

Esta teoría se desarrolla en torno al planteamiento de que la tipicidad cumple un rol desempeñado en una triple función:

Una función sancionadora, represiva para las conductas que se ubiquen dentro del tipo (tipicidad). Una función de garantía, solo las conductas que son típicas son las únicas que pueden llegar a tener una sanción. Una función preventiva; el tipo penal busca que la prohibición que contiene la ley sea para que el ciudadano no realice dicha conducta tipificada (Muñoz, 2004, pág. 200).

Por otra parte, es importante referirme a lo que en palabras del jurista Jorge Zabala expresa sobre la conceptualización de tipificación manifestando que “es la descripción de la materia de la prohibición, la realización del mismo es un indicio de la antijuridicidad de la acción”. (Zabala, 2014). Esta descripción de la acción u omisión realizada, para ser considerada como delito debe encontrarse escrita de manera puntual dentro de un cuerpo jurídico vigente y con su respectiva coerción; para emitir un juicio o sanción ya que como he mencionado que en base al principio

de legalidad si no se encuentra regulado o escrita previamente en la ley no existe tal acto como delito alguno.

4.1.3. Delito

Otro de los términos fundamentales a examinar antes de entrar en materia de la presente investigación es el delito como tal, que en palabras de Luis Jiménez de Asúa puntualiza que:

Es toda acción u omisión o comisión por omisión típicamente antijurídica y correspondientemente imputable al culpable, siempre y cuando no surja una causal de exclusión de la pena o en el enjuiciable sea susceptible de la aplicación de una medida de seguridad. (Jiménez de Asúa, 1970).

El jurista citado en su criterio de delito permite llevar a enlistar los elementos del mismo, conocidos en doctrina como la teoría del delito, existiendo tres corrientes de ella: la causalista, la finalista y la funcionalista, cada uno con diversos criterios y definiciones de los elementos; de las cual se puede de manera general y común considerar que son: acción, antijuricidad, culpabilidad y tipicidad.

Al ya haberme referido a la tipicidad anteriormente es conveniente a continuación examinar de manera breve los elementos del delito faltantes a tratar, algunos de éstos temas son de amplios debates en doctrina por cuanto para efectos de la presente investigación me limitaré a conceptualizaciones generales.

La acción: Es entendida como la realización de una conducta externa manifestada en un hecho, acto o actividad que puede ser positiva o negativa que produce cambios, es el elemento básico del delito, consistente en el comportamiento humano. Para Welzel (1951) “la acción humana es el ejercicio de la actividad finalista” (pág. 19). Es decir

que la acción se realiza con base al conocimiento causal, con una finalidad propuesta, con un movimiento corporal o físico voluntario y que bien se puede prever las consecuencias de dicha acción, a la vez que se puede proponer objetivos y plantearse la ruta de la obtención de los mismos, así como ser consciente de los resultados. La acción tiene dos fases, una interna y una externa:

La fase interna considera:

- El objetivo que se pretende alcanzar o la proposición de fines.
- Los medios que se emplean para su realización.
- Las posibles consecuencias concomitantes o secundarias que se vinculan con el empleo de los medios, que pueden ser relevantes o irrelevantes para el Derecho penal.

La fase externa considera:

- Es la puesta en marcha, la ejecución de los medios para cristalizar el objetivo principal.
- El resultado previsto y el o los resultados concomitantes.
- El nexo causal (Orellana, 2004, págs. 88 - 89).

En conclusión, el hombre para actuar o ejecutar una acción, lo realiza debido a que se planteó un objetivo y emplea medios para llegar a éste, teniendo inclusive conocimiento de las consecuencias que se pueden derivar de su accionar.

Antijuricidad: Se refiere a que la acción u omisión realizada debe estar prohibida por la ley, es de carácter valorativa hacia el acto realizado y debe perjudicar a un bien

jurídico protegido para que exista antijuricidad, va relacionada con la tipicidad, por cuanto para que un acto de acción u omisión sea calificado como punible debe estar previamente prescrito en la ley.

Welzel (1987) de otro modo lo define como “un juicio de valor “objetivo”, en tanto se pronuncia sobre la conducta típica a partir de un criterio general: el ordenamiento jurídico” (págs.76-77). La antijuricidad al igual que la acción es un acto voluntario pero que en este caso contraviene al ordenamiento jurídico con ello va a poner el peligro o a lesionar bienes que se encuentran jurídicamente tutelados. En la obra de Peña y Almanza (2010), se cita también a Bacigalupo quien sostiene que “la antijuricidad tiene por objeto establecer bajo qué condiciones y en qué casos la realización de un tipo penal (en forma dolosa o no; activa u omisiva) no es contraria al Derecho” (pág.177).

Culpabilidad: La culpabilidad es uno de los elementos más fundamentales de la teoría del delito, se refiere a las condiciones que permite declarar a alguien como culpable o responsable de un delito, considerando que la pena es la medida de la culpabilidad. La culpabilidad tiene la finalidad de ser una prevención ya que al incluirse la pena lo que busca es la resocialización del delincuente y que este produzca un efecto de prevención especial.

Sobre la estructura de la culpabilidad donde el penalista R. Frank citado por Orellana plantea que la culpabilidad no es solo una relación psicológica entre el autor y su hecho, “sino que radica en el “reproche” a ese proceso o relación psicológica, es decir, una valoración normativa (Reproche) de esa relación psicológica” (Orellana, 2004, pág. 41-42).

En conclusión, sobre el delito puedo concebir que es la conducta típica, antijurídica y culpable, como resultado de los actos externos del hombre ya sean estos positivos y negativos, que legalmente resultan imputables y dañosos a la Sociedad, implica también la puesta en peligro o lesión de bienes jurídicos tutelados, que se encuentran bajo el marco de la ley penal dado que si bien; para que esta acción sea considerada como delito debe imperar el principio de legalidad, “Nullum crime Sine Lege” no existe infracción, pena, ni proceso penal sin ley anterior al hecho.

4.1.4. Patrimonio

Considerando que los delitos informáticos afectan al patrimonio de las víctimas, es un tema que resulta conveniente tratar es por ello que expongo primero tres principales definiciones sobre ello para abarcar su origen y significado:

Procede del latín *patrimonium* y hace mención al conjunto de bienes que pertenecen a una persona, ya sea natural o jurídica. La noción suele utilizarse para nombrar a lo que es susceptible de estimación económica, aunque también puede usarse de manera simbólica (Gardey., 2013).

En otras palabras, también es entendido como el “conjunto de Derechos y obligaciones agrupados en función de una persona o fin determinado y que poseen un marcado contenido económico” (Jurídica, EnciclopediaJurídica.com, Edición 2020).

En cambio algunos autores que consideran que no se trata sólo de Derechos sino incluso de obligaciones en varios sentidos persiguiendo un objetivo expresando que:

Es un conjunto de bienes, derechos y obligaciones con los que una persona, grupo de personas o empresa cuenta y los cuales emplea para lograr sus objetivos. En ese

sentido, se pueden entender como sus recursos y el uso que se les da a estos. (Galán, 2019).

En conclusión patrimonio es toda la masa de bienes propios materiales o inmateriales de una persona o de una cierta institución, pero dicha conformación de bienes son susceptibles de un valor o utilidad económica, adquiridos de diversas formas pero que representan a su vez obligaciones, deberes y cargas en general.

4.1.5. Violación a la Privacidad de Datos

Con el manejo de las tecnologías que prestan muchos beneficios hoy en día, va implícito la manipulación de datos personales para el disfrute de dichos beneficios, como las compras en línea, pago de facturas, transferencias bancarias entre otros, desde cualquier ubicación, en cualquiera hora del día. Son estos datos los que resultan de interés para las nuevas modalidades delincuenciales.

El desarrollo de Internet y del comercio electrónico ha generado una amenaza para la privacidad de los consumidores. Internet permite a los proveedores recolectar, analizar y usar la información con gran facilidad y eficiencia. En muchos casos, sin que el propio consumidor se dé cuenta de ello. (Mok, 2010, p. 118)

Destacando la importancia que representan estos datos de carácter personal, más allá de cuestiones bancarias, la información de identificación, todo ello se considera como datos de carácter de extremo cuidado como lo menciona Villalta al definir lo que son datos personales:

Los “Datos Personales” implican toda aquella información inherente a una persona, que permiten identificarla, abarca la información que identifica o puede usarse de manera razonable para identificar a una persona en particular de forma directa o

indirecta, es decir, la información de una persona física identificada o identificable, como por ejemplo: nombre, apellidos, correo electrónico, estado civil, profesión, número de documento de identidad, entre otros. Los “Datos Personales” Sensibles, son aquellos que de divulgarse de manera indebida afectarían la esfera más íntima del ser humano o provocarle un riesgo grave, como por ejemplo, el origen racial o étnico, el estado de salud presente y futuro, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas, preferencia u orientación sexual, entre otros. (Villalta, 2017. p. 1)

Determinada la importancia de la privacidad de los datos personales, es importante referirse a la protección de los mismos, tarea no solo de cuidado de la persona titular de ellos, sino de toda la estructura estatal dentro de su deber de brindar seguridad y protección, bajo los principios y garantías establecidos en la normativa para el efecto.

En el tema de la protección de la información personal se reconoce la existencia de una serie de principios generales, garantías y excepciones. Los principios generales son esenciales para garantizar, en forma directa, la adecuada protección de la información personal (y, en algunos casos, los intereses legítimos de personas jurídicas), e indirectamente, para salvaguardar los derechos a la privacidad, al honor, a la reputación, a la libertad de expresión (incluyendo la libertad de prensa), entre otros; mediante la generación de un adecuado marco jurídico en donde puedan hacerse efectivos todos y cada uno de estos derechos y garantías fundamentales del hombre. (Mok, 2010, p. 116)

Como resulta evidente la violación de datos personales, lleva a un perjuicio de incalculable valor dado que es una puerta abierta para varias afectaciones, como lo

señala la autora citada, pueden ser utilizados para atentar contra el honor de un persona y sin duda contra su patrimonio. Es por ello que al igual que la autora citado considero necesario tener una legislacion en este caso penal, que contemple todas las modalidades delictivas que se desarrollan hoy en dia por el avance tecnologico, los datos personales representan información de gran valor para cada sujeto, por lo que resulta muy ambicionado por estafadores y ladrones de identidad.

4.1.6. Estafa

Según el diccionario de la Real Academia Española, estafa “es el delito que se comete, con ánimo de lucro, utiliza engaño bastante para producir error en otro, reduciéndolo a realizar un acto de disposición en perjuicio propio o ajeno” (Real Academia Española RAE; Consejo General del Poder Judicial, 2016).

Remontando a su origen el término estafa, proviene de voces latinas *stellionatus* que significa “el estelión o salamandra”. El maestro Carrara, citado por Freyre, hace una explicación sobre el *stellionatus* y afirma “El *stellionatus* o salamandra, animal de colores indefinibles, pues varía ante los rayos del sol, surgió a los romanos el nombre de *estelionato* como título de delito aplicable a todos los hechos cometidos en perjuicio de la propiedad ajena, que fluctúan en el hurto, que, aunque participen de las condiciones y de otro delito, no son precisamente ni uno ni el otro” (Carrara, 1980, pág. 426).

Con las palabras de este jurista se da luces acerca que el estudio del delito de estafa ha venido desde la aparición del Derecho Romano, con un fundamento muy claro que es: la estafa es el fraude con el fin de perjudicar el patrimonio ajeno.

En la actualidad se mantienen los criterios del Derecho Romano, facilitando la definición de estafa, en palabras simples como el perjuicio al patrimonio de una

persona. Este delito se encuentra formando parte de los delitos contra la propiedad, encontrándose diferenciado del hurto, de la extorsión, de la apropiación indebida; por la doctrina y la jurisprudencia.

Concretamente la estafa es un delito que, recurriendo al engaño producido por parte del estafador, hacía la víctima induce a esta al error; aprovechándose de su buena voluntad o su necesidad, con la finalidad de obtener un fin de lucro en su beneficio y a la vez afectando su patrimonio. Entonces se puede decir que la estafa presenta dos aspectos importantes como es el engaño y el daño al bien patrimonial.

Es fundamental tener presente estos aspectos mencionados a lo largo del desarrollo de la presente investigación, considerando que el delito de estafa es netamente ejecutado en contra el patrimonio y propiedad. El tipo de estafa más común es la promesa de entregar algo que no existe, pero antes de la supuesta entrega se ha pedido un anticipo y finalmente la persona que entregó ese anticipo nunca recibió el bien o cosa prometido.

Este delito, se ve caracterizado por el hecho de ocultar o mentir con información que le permita obtener un beneficio a costa del daño económico y a la vez patrimonial a otra persona, ya que el estafador se encuentra guiado por su único fin que es el conseguir un beneficio económico para sí mismo.

4.1.7. Tecnologías de la Información y la Comunicación

Es importante describir y conocer sobre las tecnologías de la información y la comunicación, para efectos y comprensión de este estudio. Primero he de referirme al término tecnología, que se entiende como el conjunto de conocimientos científicos y técnicas para crear o desarrollar productos tecnológicos o a la vez desarrollar ideas,

con la finalidad de solucionar un problema concreto, se da como respuesta al deseo del ser humano de transformar o cambiar su calidad de vida.

Por otro lado, en cuanto a la información, es entendida como la integración de datos de una manera ordenada que constituyen un mensaje en concreto sobre un fenómeno o ente, y a través de esta se aporta significado o sentido a las cosas, para la solución de problemas o toma decisiones que más se adapten a nuestra necesidad, o para incrementar el conocimiento sobre algo en concreto. Y finalmente la comunicación es el proceso de compartir, intercambiar o transmitir mensajes, información o significados entre dos o varias personas, permitiendo de esta manera establecer un tipo de relación social dentro de una comunidad o Sociedad, y se la puede realizar de manera oral, escrita, gestual o por medio de sonidos.

En la actualidad gracias a los avances tecnológicos y científicos se han desarrollado un sin número de canales o medios de comunicación para el uso y disponibilidad de todas las personas en general, permitiendo estar comunicados en tiempo real sin importar la distancia en la que se encuentren. Entre las múltiples definiciones de las Tecnologías de la Información y la Comunicación es de relevancia citar que:

En líneas generales podríamos decir que las nuevas tecnologías de la información y comunicación son las que giran en torno a tres medios básicos: la informática, la microelectrónica y las telecomunicaciones; pero giran, no sólo de forma aislada, sino lo que es más significativo de manera interactiva e inter-conexionadas, lo que permite conseguir nuevas realidades comunicativas. (Cabero, 1998, pág. 198).

Erróneamente se puede llegar a entender que las TIC es solo un tema de asunto, que únicamente le compete a la área o materia informática, más en la realidad se involucra a otras materias como las ciencias sociales y la política. Si bien desde el

punto de vista informático se define a las TIC como “conjunto de técnicas, desarrollados y dispositivos avanzados que integran funcionalidades de almacenamiento, procesamiento y transmisión de datos” (Moscoso, pág. 1), desde otro punto de vista como hemos visto las Tecnologías de la Información y la Comunicación, también hacen referencia al desarrollo de la Sociedad, organización y gestión empresarial.

Para el redactor colombiano de la revista Hallazgos William Díaz las Tecnologías de la Información y la Comunicación son:

El conjunto de herramientas, soportes y canales desarrollados y sustentados por las tecnologías (telecomunicaciones, informática, programas, computadores e internet) que permiten la adquisición, producción, almacenamiento, tratamiento, comunicación, registro y presentación de informaciones, en forma de voz, imágenes y datos, contenidos en señales de naturaleza acústica, óptica o electromagnética a fin de mejorar la calidad de vida de las personas. (Díaz, 2013, pág. 213-233)

La Universidad Nacional Autónoma de México en su definición de las Tecnologías de la Información y la Comunicación (TIC) ejemplifica a los soportes tecnológicos a las “computadoras, teléfonos móviles, televisores, reproductores portátiles de audio y video o consolas de juego” (Universidad Nacional Autónoma de México , 2018), ya que todos éstos integran redes, medios informáticos y de telecomunicaciones.

La Unesco por su parte en cambio define a estas como el conjunto de “disciplinas científicas, de ingeniería y de técnicas de gestión utilizadas en el manejo y procesamiento de la información: sus aplicaciones; las computadoras y su interacción con hombres y máquinas; y los contenidos asociados de carácter social, económico y cultura” (Unesco, 2002)

Entre otra de las definiciones más importantes y que no es posible de obviar es la de Cobo Romaní, ya que define a las tecnologías de la información y la comunicación como:

Dispositivos tecnológicos (hardware y software) que permiten editar, producir, almacenar, intercambiar y transmitir datos entre diferentes sistemas de información con protocolos comunes. Integran medios de informática, telecomunicaciones y redes, posibilitan la comunicación y colaboración interpersonal y la multidireccional (uno a muchos o muchos a muchos). Desempeñan un papel sustantivo en la generación, intercambio, difusión, gestión y acceso al conocimiento. (Cobo Romaní, 2011).

Las tecnologías de la información y la comunicación o también conocidas como nuevas tecnologías de acuerdo a las definiciones de distintos autores son un conjunto de sistemas, instrumentos, soportes y canales tecnológicos (hardware, telecomunicaciones, software, informática e internet) desarrollados y sustentados por las tecnologías, que permiten procesar, almacenar, registrar presentar información en forma de imágenes, datos o de voz, y la interacción entre hombres y máquinas. Toman un papel muy importante en el desarrollo social, económico y cultural en la generación, difusión y acceso al conocimiento dentro una Sociedad.

Estas herramientas tecnológicas permiten un mejor acceso, clasificación y selección de información para realizar una actividad ya sea de forma individual o colectiva, y al permitir este tipo de actividades también posibilita que personas inescrupulosas inventen nuevas modalidades de cometer actividades ilícitas en contra del patrimonio de las personas por el acceso libre a ellas.

4.1.8. Estafa Informática

Según el diccionario de la Real Academia Española, al respecto de la estafa informática otorga la definición más sencilla acerca de este delito declarando que “es el delito de estafa que se comete por medios informáticos” (RAE, 2019).

En términos más amplios puedo exponer que la estafa informática existe cuando un agente o sujeto de manera astuta obtiene cierto provecho mediante el uso de mecanismos de conexión de forma autorizada por la computadora obteniendo datos informáticos no autorizados, con ellos se conocen ciertas circunstancias delicadas de los clientes o usuarios perjudicando pérdidas y afectaciones en su patrimonio. Gustavo Eduardo Abozo y María Florencia Zapata con respecto a la estafa informática sostienen que:

Los tipos penales especiales de estafa informática (Computer Betrug) regulan este tipo de comportamientos donde no media engaño o error alguno, sino un uso no autorizado por parte del interesado por lo que se ha generado la necesidad de regular, a la par de la previsión de la estafa genérica, otra que atienda de manera exclusiva a la mediación de un aparato mecanizado (Abozo, & Zapata 2006, pág. 89).

Camacho Losa presenta las notas del fraude informático: 1. una conducta fraudulenta (no profundiza en lo que deba entenderse por fraudulento), que consiste en un uso indebido o una manipulación fraudulenta de elementos informáticos; 2. la presencia de los componentes físicos y / o lógicos del sistema informático como instrumento de auxilio de la conducta; 3. la finalidad perseguida de obtener un beneficio ilícito (elemento subjetivo que se concreta en el ánimo de lucro injusto); 4. la producción de un perjuicio en otro. Este elemento aparece matizado por el propio autor al apuntar que puede no consistir en un perjuicio económico cuantificable. (Camacho, 1987).

Por su parte, Romeo Casabona, describe el fraude informático (que inicialmente denomina «manipulación de datos informatizados») como “la incorrecta modificación del resultado de un procesamiento automatizado de datos, mediante la alteración de los datos que se introducen o ya contenidos en el ordenador en cualquiera de las fases de su procesamiento o tratamiento informático, con ánimo de lucro y en perjuicio de tercero”. (Casabona, 1987).

También se entiende por estafa informática a “quien con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro ”. (- Caso 2422/2011, Sala Segunda, de lo Penal, 2012, Valencia).

De los conceptos antes expuestos puedo definir que, a la Estafa Informática como un delito de estafa cometido a través de medios informáticos o por medio del internet que son parte de las tecnologías de la información y la comunicación (redes sociales, correos electrónicos, mensajes de textos, llamadas de voz, etc.). Al igual que el delito de estafa común, existe el engaño para inducir al error a una persona, pero no se puede decir que la computadora engañó a una persona si no que debe existir manipulación o alteración, de los medios electrónicos para que se cumpla el cometido de las personas que realizan esta conducta.

4.2. Marco Doctrinario

4.2.1 Las Tecnologías de la información y la Comunicación Tics en un mundo globalizado

En un mundo globalizado la tecnología toma un papel muy trascendental en el desarrollo y progreso de la Sociedad, al igual que la comunicación desempeña un rol fundamental en la vida del ser humano en respuesta a la necesidad de intercambiar

información, ideas, datos, proyectos etc., y conforme nos enfrentamos a la modernización de la Sociedad, la forma de comunicarse evoluciona.

La interacción entre máquinas y humanos ha demostrado que permite el desarrollo social, económico, cultural y empresarial, el almacenamiento, registro procesamiento y en equipos informáticos, instrumentos de transmisión y recepción de información y de comunicación; como es la telefonía móvil, fija, radio y televisión, así como en sistemas informáticos y computadoras son parte de todo este gran conjunto de las tecnologías de la información y la comunicación. No se puede dejar de lado a una de los más grandes avances de la tecnología y muy popular hoy en día; el internet cambió por completo la forma de comunicarse revolucionando el uso de mensajería a través de correos electrónicos, chat o mensajería en tiempo real ya sea desde un teléfono móvil o un ordenador. Además, que conduce a toda una nueva generación de términos y conceptos nuevos entre los principales: redes, terminales y servicios siendo estos tres la principal clasificación de las Tecnologías de la Información y la Comunicación.

La importancia de esta revolución tecnológica de esta red de redes con tan alto impacto se debe a que:

Simultáneamente, la difusión a escala planetaria de las nuevas tecnologías de la información y comunicación (TIC) y de las redes informáticas, ha puesto en marcha un proceso de conectividad sin precedentes en la historia humana, el cual ha permitido multiplicar las posibilidades de generar y socializar información y conocimiento, eliminando progresivamente las barreras espacio- temporales (Yáñez & Villatoro S, 2005, pág. 7).

En las actas del II Seminario Internacional de Cooperación y Desarrollo en Espacios Rurales Iberoamericanos con la asistencia de grandes autores se hace alusión a las Tecnologías de la Información y la Comunicación, expresando que:

Se ha señalado que las nuevas TIC constituyen herramientas fundamentales para facilitar el acceso a conocimiento y potenciar las capacidades de innovación de los países de América Latina y el Caribe, y así lograr que éstos puedan integrarse plenamente al mundo globalizado (Hopenhayn y Ottone, 2000, pág. 96).

Ciertamente son una promesa que no restringe a ningún campo dado que tiene muchos ámbitos de aplicación entre ellos se puede mencionar el fomento de la democracia, la prestación de servicios con una mayor eficiencia ya sean estos públicos o privados, o una mejoría en cuanto a la calidad de educación, entre otros. Si bien, es un progreso tecnológico proveedor de grandes beneficios no deja de ser un reto y un tema de amplio debate debido a aspectos y situaciones que se derivan de este y para el cual tanto el Estado, empresas, instituciones y el mismo ciudadano están descubriendo y explorando los límites de esta red. Juan Rojo Ponente del tema Presentación del panel “El rol de las tecnologías de la información y comunicación (TIC) en las experiencias de institucionalización de la política social” recopilado en la obra de Yáñez & Villatoro, al respecto manifiesta que:

Por su parte el Estado y las instituciones se ven presionados por el desarrollo de nuevos sistemas en línea para el monitoreo y evaluación de programas y políticas públicas, así como sistemas expertos para la toma de decisiones. Los nuevos gerentes públicos no sólo deben decidir ahora sobre las políticas en sus áreas de competencia, sino que también se ven obligados a tomar decisiones sobre la incorporación en la

organización de nuevas tecnologías de información y comunicación (Yáñez & Villatoro S, 2005, pág. 12).

Las características que diferentes autores especifican como representativas de las Tecnologías de la Información y la Comunicación, recogidas por Cabero, en resumen, son: “inmaterialidad, interactividad, interconexión, instantaneidad, digitalización, mayor influencia sobre los procesos que sobre los productos, penetración en todos los sectores (culturales, económicos, educativos, industriales...), innovación, tendencia hacia automatización, diversidad y almacenamiento” (Cabero 1998, Pág., 200). Con todos estos antecedentes se observa que estamos vivenciando un cambio de paradigma dadas todas estas características y posibilidades que ofrecen las Tecnologías de la Información y la Comunicación, como herramienta para acceder a información, a recursos y servicios.

4.2.2 Avances de la Tecnologías de la Información y la Comunicación

La comunicación entre los seres humanos durante el transcurso de los años, ha ido sufriendo grandes transformaciones frente a su necesidad de comunicación, siendo esta la forma de intercambiar ideas, de dar a entender mensajes sentimientos; cumpliendo así la finalidad de darnos a entender con nuestros semejantes. Los términos tecnología de la información y la comunicación lleva asociar rápidamente a otros términos como computadora y tecnología, pero en la actualidad los términos iniciales se han expandido y comprende muchos otros entre ellos; directamente las tecnologías de la información, tecnologías de comunicación, ciencias de la información, reconocimiento de patrones, procesamiento de datos, minería de datos, transformación de datos, redes de computadores, gravamen de tecnología, criptografía, gobierno, telemática, gerencia de sistemas, entre otros.

Es así que retomando una parte fundamental de esta acción de intercambiar información ha provocado que los métodos y recursos de comunicación vayan evolucionando; desde tiempos rudimentarios se utilizaba diferentes medios de comunicación tales como el chasqui, envío de mensajes mediante aves, el uso de pergaminos, la invención del telégrafo. Otra de las formas más antiguas de comunicación es el periódico que “se inicia con los medios escritos o pictóricos: pinturas sencillas hasta luego formar conjunto de signos llegando a ser conocidos como alfabetos” (Quezada, 2010, pág. 118). Es así que el periódico en la era industrial fue el mayor medio de comunicación desarrollado y el más popular, actualmente los periódicos no han perdido del todo su espacio entre los medios de comunicación, la mayoría de ellos además de su versión impresa tiene disponible una versión digital en internet, siendo esta última la característica de estar a un bajo costo y a un fácil acceso. En sí el término tecnología de la información se empieza a utilizar en la década de los años 70 ocurriendo así toda la lista de acontecimientos producidos a lo largo de la historia.

Ya para los años 80 un evento que marcó específicamente el año de 1843 es la invención de la radio raíz de la comunicación inalámbrica. “Esta tecnología transmite señales, modulando ondas electromagnéticas, y lo más importante, el medio que utiliza para propagarse es el aire” (Quezada, 2010, pág. 119). A este evento le siguió el sistema de transmisión y recepción de imágenes fijas o en movimiento con sonido la conocida televisión que específicamente en el año de 1884 se efectuaron las primeras transmisiones.

El otro salto de la tecnología de la comunicación, es la creación de las primeras computadoras lo que para 1945 en cuanto al mejor desarrollo de tecnología significa

tener un “armamento que operaba a larga distancia, los computadores calcularían las trayectorias de proyectiles submarinos y aéreos. Formas de comunicación más seguras y la posibilidad de descifrar los mensajes enemigos” (Quezada, 2010, pág. 120). Junto a esta evolución el internet las acompañó como medios modernos para la comunicación. Vale no olvidar a la telefonía móvil o celular que un teléfono alámbrico se pasó a un sencillo dispositivo que no solo ofrece llamadas de voz, sino que posee una gran variedad de actividades. Pero aun así el internet camina a la par de estos siendo el internet la evolución más sorprendente:

Comenzó como una red para compartir información entre investigadores y esta información se limitaba a mensajes de texto en crudo. Poco a poco se empezó a compartir archivos de imágenes y texto enriquecido. Luego se extendió a esta posibilidad a compartir cualquier tipo de archivo, aunque la velocidad de la red era muy limitada pero rápidamente aparecieron mejores medios para aumentar la velocidad y que se vuelva más accesible al público (Quezada, 2010, pág. 131).

El gran paso que da la tecnología es la inclusión de la informática a las comunicaciones, con ello se empieza hablar de las Tecnologías de la Información y la Comunicación, y su era digital moderna. La innovación y las transformaciones tecnológicas son de gran importancia para el desarrollo económico y social, a medida que en la Sociedad surgen nuevas necesidades, hoy en día el uso de la Tecnologías de la Información y la Comunicación, son de uso cotidiano ya que ha permitido la automatización de procesos académicos, administrativos, económicos y entre los que cabe resaltar y para ejemplificar por la materia de estudio de la presente investigación son en el ámbito judicial, ya que a través del sistema SATJE creado por la función judicial facilita la consulta del estado de procesos tanto a la parte acusada

por a la acusadora como a las Sociedad en particular, es así que con la transformación de las tecnologías hoy en día es de fácil alcance para los interesados como a los profesionales del derechos en ejercicio que se les permite tener su casillero electrónico y con ello la obtener información requerida tan solo con un clic, encontrándose a un fácil alcance de la información y como ventaja adicional el ahorro tiempo y recursos económicos a todo el sistema judicial.

4.2.3. Tipos de Tecnologías de la Información y la Comunicación

4.2.3.1. Redes

Los avances producidos en las redes dentro de las tecnologías de la información y la comunicación han sufrido un desarrollo a lo largo de las últimas décadas. Entre lo que se puede exponer acerca de lo que es una red se puede a citar que "Una RED es un conjunto de equipos conectados entre sí por medio de un cable u otro medio físico con el fin de compartir recursos" (Telefonía fija y móvil, Banda ancha, Televisión, Satélites, etc.). (Blogspot, 2012)

En otras palabras, se denomina red a todo o cualquier sistema de comunicación que cumple la misión de enlazar dos o más equipos, siendo posiblemente estos unos computadores, celulares, etc. En materia de informática se indica que una red se conforma con 3 componentes que son: usuarios, software y hardware.

Las redes así constituidas, no son sólo una estrategia para la cooperación y construcción del conocimiento, sino que son el modelo organizativo que puede contribuir al fortalecimiento institucional al integrarse como redes generadoras de conocimiento y que parten de la unidad que conforma un cuerpo” (Beltrán, Hernández, & Carbajal , 2012, pág. 33).

Como he tratado en el desarrollo de este trabajo de investigación, las redes son parte de toda la revolución de las tecnologías de la información, en paralelo con el surgimiento del internet; lo que todo esto inspira un modelo organizativo para la Sociedad.

La ventaja que proporcionan las redes en la actualidad es la de compartir recursos que normalmente son poco utilizados o que tienen un alto costo para el usuario como por ejemplo las impresoras. Compartir e intercambiar información con esto los usuarios no trabajan de forma aislada, debido a los mecanismos sencillos existentes para intercambiar información de gran volumen. Otra de las ventajas que se obtiene de las redes son la mayor efectividad que brindan, es decir la capacidad de organizar varios recursos considerando que, además de compartirlos se necesita menos recursos; resultando ser óptimos en los presupuestos de las empresas.

En las redes se distinguen algunos tipos categorizados según su tamaño, su velocidad de transferencia de datos y el alcance de datos que tienen. Generalmente las tres categorías principales son: la conocida red de área local o LAN, la red de área metropolitana o MAN y finalmente la red de área extensa o WAM.

Entonces puedo concluir que las redes son el medio para compartir recursos, que conforman parte de las tecnologías de la información formando parte de las herramientas de crecimiento y evolución.

4.2.3.2. Terminales

Los terminales son conocidos como consola, este es un dispositivo electrónico o electromecánico de hardware que es usado con la función de introducir datos para ser mostrados en una computadora. Es conceptualizado por los expertos como "Un terminal, conocido también como consola es un dispositivo electrónico o

electromecánico de hardware, usado para introducir o mostrar datos de una computadora o de un sistema de computación" (Blogspot, 2012) Televisores, Computadores de escritorio y portátiles, Teléfonos móviles o Smartphone, Software y sistemas operativos, etc.

Existen varios terminales o en otros términos dispositivos que conforman las Tecnologías de la Información y la Comunicación, puedo enlistar que estos son: el ordenador, el navegador de internet, los sistemas operativos para ordenadores, los teléfonos móviles, los televisores, los reproductores portátiles de audio y video o las consolas de juego. Entonces se puede indicar que los terminales actúan como un punto de acceso a la información y son uno de los elementos que continuamente evolucionan.

Para algunos autores y expertos en el tema consideran que los terminales son dispositivos de entrada y salida justificando su percepción en que: algunos dispositivos de entrada más corrientes actualmente se encuentran los terminales; que se utilizan para transmitir datos al ordenador (son el medio de comunicación entre el usuario y el ordenador). Un terminal está formado por un teclado y una pantalla: el teclado permite introducir programas o datos al ordenador (Roig, 2008, pág. 16).

La importancia de los terminales yace en que el funcionamiento de un hardware lo expande y siendo el computador es el principal hardware en la Sociedad; los terminales se enfocan en ampliar sus funciones con el fin de mejorar las actividades cotidianas como la búsqueda de información. Es así que los terminales modernos son utilizables de diversas maneras, dado que un terminal puede emular hasta 40 o 50 máquinas simultáneamente lo que lleva a que el usuario utilice un sitio de trabajo.

4.2.3.3. Servicios

Las Tecnologías al ser condicionadas por la evolución y la forma de acceder a los contenidos, servicios y aplicaciones disponibles hoy en día a medida que se extiende la banda ancha, se producen cambios en los servicios.

Según Serralde los servicios en las tecnologías han ido evolucionando. Al principio los servicios estaban centrados en la difusión de información estática y algunas otras herramientas. Luego aparecieron un segundo grupo de servicios como el comercio electrónico, la banda online, el acceso a contenidos informativos, de ocio y el acceso a la administración pública (Serralde, 2010)

Es conveniente hablar de servicios en las Tecnologías de la Información y la Comunicación donde se mantiene un modelo de proveedor-cliente todo en función de mecanismos tecnológicos, por medio de las Tecnologías de la Información y la Comunicación, se ofrecen varios servicios a los consumidores.

Los servicios más importantes que ofrece los tics son: el correo electrónico, la búsqueda de información, la banca online, el audio y música, la televisión y el cine, el comercio electrónico, administración y gobierno, la e-sanidad, la educación, los videojuegos y los servicios móviles.

Para finalizar es de considerar que se concibe también como un servicio a un software que sea utilizado para realizar alguna actividad como compras o realizar pagos; en cambio otra forma de servicios con las Tecnologías de la Información y la Comunicación, es el brindar utilidad como en el caso de los envíos de paquetes si bien las Tecnologías de la Información y la Comunicación, no desempeñan la actividad principal, pero son usadas para el registro y verificación de los estados de envío.

4.2.4. Elementos que configuran el delito de Estafa Común

Para que se configure el delito de estafa es necesario que contenga los siguientes elementos:

Engaño; Error, que ese engaño produzca a la víctima; Disposición patrimonial (acto que genera perjuicio) que provoca el autor del delito mediante su engaño; Perjuicio patrimonial que sufre una persona y además es necesario que exista una relación causal entre el engaño y el perjuicio patrimonial (MisAbogados.com, 2016).

Para que se configure el delito de estafa debe existir dolo, conciencia y voluntad de engañar a otro, produciéndole un perjuicio patrimonial a él mismo o a una tercera persona además debe contener los siguientes elementos:

- ✓ Un engaño “precedente o concurrente” a la defraudación: Es decir, que lo primero que tiene que suceder para que haya un delito de estafa, es que una persona engañe a otra. Pero, no basta con cualquier engaño, sino que: Dicho engaño ha de ser «bastante», suficiente y proporcional para que la persona que engaña pueda conseguir el fin que se ha propuesto.

Este engaño con las características de ser idóneo y eficaz ha de producir un error en el sujeto pasivo, en el cual se vicie su voluntad para que se efectúe ciertos hechos planteados por el sujeto activo del delito. Ocasionando así un desplazamiento patrimonial en el sujeto pasivo; este sufre una disminución de sus bienes o un perjuicio de lesión a sus intereses económicos por el efecto de maniobras falaces, es decir, estas maniobras son siempre enfocadas al lucro propio o de un tercero.

- ✓ Error esencial en el sujeto pasivo: el siguiente paso para construir un delito de estafa, es que el engaño, que como he dicho, ha de ser bastante y provoque un error en la persona. Es decir, que el error ha de estar totalmente conectado con el

engaño anterior, porque el engaño ha creado un conocimiento deformado o inexacto de la realidad. Esto hace que la persona víctima del engaño actúe bajo una falsa presuposición de que la otra persona le ha manifestado la verdad.

- ✓ Acto de disposición patrimonial: como consecuencia del engaño, que a su vez ha causado un error en la persona, tiene que producirse la entrega de un bien de forma voluntaria, que conlleva de forma directa la producción de un perjuicio patrimonial.
- ✓ Ánimo de lucro: lo que quiere la persona que engaña es lograr un beneficio a costa de la persona engañada, por tanto, el perjuicio que se causa a una y el beneficio que logra la otra están íntimamente relacionados. (Penalistas, s.f.).

Los medios empleados: Los medios que caracterizan al delito de estafa son:

- El nombre falso
 - La falsa calidad
 - Los manejos fraudulentos
 - La existencia de falsas empresas
 - Existencia de un poder falso o crédito imaginario.
- ✓ Bien Jurídico Protegido: En este tema es de hablar del ataque a un elemento integrante del patrimonio (propiedad, posesión, Derecho de crédito, etc.), se constituye en estafa cuando de este se derivan una disminución del valor del patrimonio considerado se reste.

En conclusión, el delito de estafa tiene como fundamento perjudicar el patrimonio de otra persona, el cual debe reunir todos los elementos que en nuestra legislación se plantea en el Artículo 186 ya anteriormente referido.

4.2.5. Delitos Informáticos

Como el avance tecnológico ha impulsado a la Sociedad en todos los aspectos posibles, mejorando la comunicación y miles de servicios más, esta misma globalización arrastró consigo y desarrollo un nuevo escenario para la Sociedad al que enfrentarse; los delitos informáticos. Se encuentra tantos conceptos acerca de los delitos informáticos de varios investigadores del tema, algunos de los cuales es de relevancia citar a continuación:

Entre estos Julio Téllez Valdés conceptualiza al delito informático en una forma típica y atípica, entendiendo por la primera a “las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin” y por las segundas “actitudes ilícitas en que se tienen a las computadoras como instrumento o fin” (Valdés, UNED, 1966).

María Cinta Castillo entienden que "delito informático es toda acción dolosa que provoca un perjuicio a personas o entidades en cuya comisión intervienen dispositivos habitualmente utilizados en las actividades informáticas" (Castillo M. C., 1989).

En resumen, los delitos informáticos son aquellas actividades y conductas ilícitas susceptibles de ser sancionadas que se cometen mediante el uso de computadoras, sistemas informáticos u otros dispositivos de comunicación que tienen por objeto causar daños haciendo un uso indebido de estos medios informáticos, concluyendo así que la informática no deja de ser un medio o instrumento para realizar un delito.

El convenio sobre Ciberdelincuencia celebrado en Budapest el 23 de noviembre del 2001, con el objeto de proteger a la Sociedad frente a la ciberdelincuencia en particular por los profundos cambios provocados por la digitalización, la

convergencia y la globalización. Las Tecnologías de la Información y la Comunicación y la información que éstas contienen, ponen en riesgo a la Sociedad en general de ser víctimas de delitos informáticos entre estos el delito de estafa informática en su Artículo 8 establece que “tipificar como delito en su Derecho interno los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante: a.- cualquier introducción, alteración, borrado o supresión de datos informáticos; b.- cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona.” (Europa, 2001)

Es importante resaltar que los delitos informáticos que en la actualidad constituyen uno de los delitos que más han evolucionado, por lo cuando los cuerpos legales deben ir a la par de estos adelantos, teniendo en cuenta que mediante esta nueva forma delincencial se afecta a la integridad personal y convierte a los usuarios de la informática en víctimas de una gran afectación psicológica y en algunos casos patrimonial.

El número de posibles delitos informáticos es demasiado amplio y su única limitación existente es la imaginación de su autor y su capacidad técnica. Por desgracia “se producen muchos ilícitos informáticos que puedo considerar que son fraudes pero que nunca podremos calificar como delitos”. (Ignoto Azaustre, Fernández Sánchez, Lucero Manresa, Navarro, & Ramos González, 2001, pág. 162). Estas palabras no pueden ser más acertadas a la realidad actual dado que si bien, hay estas acciones u omisiones ilícitas derivadas o realizadas por medios informáticos no son consideradas como delitos debido a que no los encontramos señalados legalmente como una conducta tipificada en la ley penal. Los delitos informáticos si

configuran conductas que son socialmente reprochables y no se encuentran en nuestro ordenamiento jurídico con una correcta recepción legislativa que encierre a estas conductas en la categoría de delitos. “La persecución de tales delitos encuentra una valla infranqueable en el principio constitucional de Nullum crimen, nulla poena sine lege previa, lo que conlleva a su no punición en el ámbito jurisdiccional, provocando la impunidad de tales conductas” (Zarich, 2005, pág. 155).

Entre las definiciones de delitos informáticos resulta interesante considerar las palabras Téllez (1996) que refiriéndose concretamente a la situación mexicana frente a los delitos informáticos señala que no es fácil dar un concepto de este tema debido a que:

En razón de su misma denominación alude a una situación muy especial, ya que para hablar de “delitos” en el sentido de acciones típicas, es decir, tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión “delitos informáticos” este consignada en los códigos penales, es decir, haya sido objeto de tipificación (Valdés, Derecho Informático, 1996, pág. 103).

En un sentido más amplio el autor señala que se pueden formar varios grupos de figuras delictivas y que son claramente diferenciadas: “Delito informático propiamente dicho, protección del Derecho a la intimidad, propiedad intelectual informática, acciones físicas contra la integridad de los ordenadores, los hackers, los virus informáticos, la sustracción de tiempo de ordenador” (Ignoto Azaustre, Fernández Sánchez, Lucero Manresa, Navarro, & Ramos González, 2001, pág. 162).

Existen diferentes clasificaciones de los diferentes delitos informáticos; entre ellas las de Parker que a pesar del tiempo en que la hizo mantiene aspectos que la hacen aún estar en vigencia:

1. Introducción de datos falsos (data didding).
2. Caballo de Troya (Trojan Horse).
3. Técnica de Salami (Salami techniques o Rouding down).
4. Uso no autorizado de un programa (Superzapping).
5. Trampas (Tramp Doors).
6. Bombas lógicas (Logic Bombs).
7. Ataques asincrónicos (Asynchronous Attaks).
8. Recogida de información Residual (Scaveging).
9. Filtración de datos (Data Leakage).
10. Trasego de personas (Piggybacking and Impersonation).
11. Pinchado de líneas (Wiretapping).
12. Simulación y moldeado de delitos (Simulation and modeling).

Según el Convenio Sobre La Ciberdelincuencia del consejo de Europa de noviembre de 2001 los clasifica Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:

- a) Acceso ilícito: cuando se accede a un sistema informático infringiendo las medidas de seguridad con la finalidad de obtener datos u otra intención delictiva. Por ejemplo, las aplicaciones móviles maliciosas para robar información de Smartphones.
- b) Interceptación ilícita de datos: que por medios tecnológicos se intercepte de forma deliberada e ilegítimamente datos informáticos comunicados confidencialmente mediante un sistema informático.
- c) Interferencia en los datos: comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos.

d) Interferencia en el sistema: quien obstaculice grave, deliberada e ilegítimamente el buen funcionamiento de un sistema tecnológico o informático por medio de la introducción, transmisión, promoción de daños, borrado, deterioro, alteración o supresión de los datos informáticos.

e) Abuso de los dispositivos: producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de un dispositivo o un programa informático que haya sido diseñado para la comisión de un delito informático. De igual manera si se trata de una contraseña, código de acceso o datos informáticos similares que permitan acceder a la totalidad o parte de un sistema informático con el fin de ser utilizados para cometer un delito.

La revista digital Parlar el 22 de diciembre del 2019 publicó datos estadísticos de los delitos informáticos en Ecuador. Las primeras cifras alarmantes son en las dos modalidades más comunes de acceder al sistema informático de una persona, que primero es por abandonar algún dispositivo con información sensible y el segundo por aceptar a desconocidos en redes sociales lo que muchas veces son los mismos piratas informáticos que se aprovechan del desconocimiento en la ciudadanía de estos riesgos existentes en el uso de la informática. Otro de los datos relevantes son los que señalan a Guayaquil como la ciudad donde más se registran estos tipos de delitos, seguido por Pichincha y Azuay.

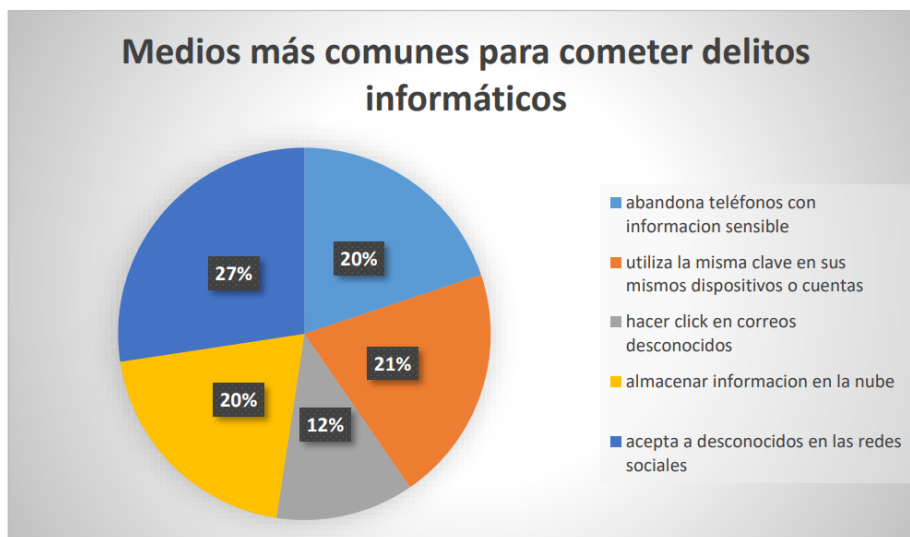


Ilustración 1 Ilustración 1 Revista Parlar, Medios comunes para cometer delitos (Redacción Justicia 2016)

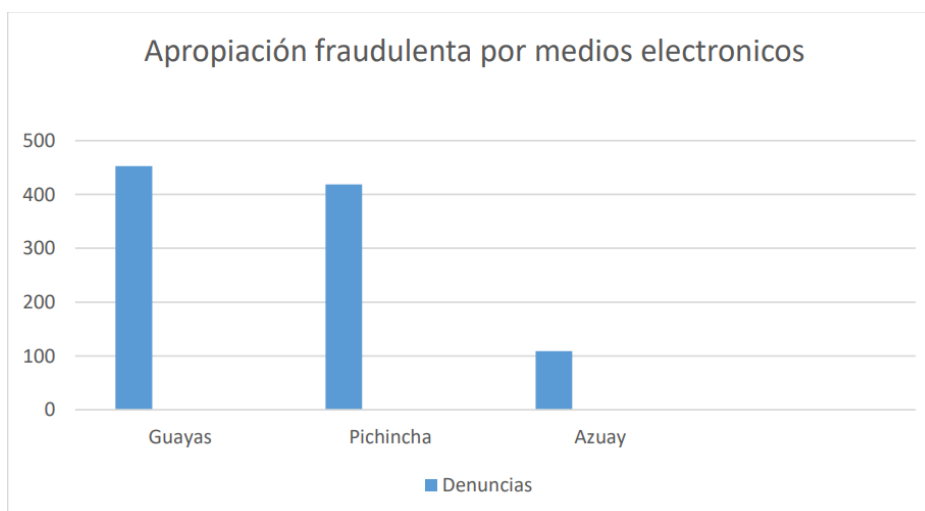


Ilustración 2 Revista Parlar, Denuncias Fiscalía 2018

El aumento de estas cifras puede darse al considerar que existen cifras vacías, es decir, las personas que nunca presentaron la denuncia ya que sienten que no se dará ningún tipo de seguimiento por las autoridades, por cuanto prefieren abstenerse de denunciar su afectación. Considero además que, actualmente en nuestro país carecemos de técnicos que asuman la función de hacer peritajes en la red para descubrir estos nombrados “piratas cibernéticos” y vincular dichas acciones a delitos

informáticos; a esta inseguridad se debe sumar el que la legislación mantiene vacíos en cuanto a delitos informáticos.

4.2.6.1. Elementos del delito informático

4.2.6.1.1. Sujeto pasivo

Al hablar del sujeto pasivo del delito, me refiero a el sujeto sobre quien recae la conducta delictiva, en palabras más concretas se trata de la víctima del delito que ya en casos de los informáticos el delito recae sobre la base de datos de personas ya sean naturales o jurídicas.

El Derecho Español, afirma que la conducta del sujeto pasivo, guiada por el ánimo de lucro, se dirige a una "provocación de una disposición y de un perjuicio patrimonial, pero en la que el mecanismo defraudatorio no es propiamente la provocación mediante engaño de un error de la víctima, sino la manipulación de un sistema informático -de sus datos o de su modo de procesamiento- conformado según la voluntad de la víctima.

En la estafa informática no se ejerce violencia en las personas ni fuerza en las cosas, hay una manipulación informática y como consecuencia de ello, al igual que en el hurto, se produce una transferencia, una sustracción, un apoderamiento y finalmente, ese apoderamiento lo es de un bien mueble como es el dinero, sin el consentimiento de su dueño.

Existe una cierta evolución en la actualidad en cuanto a denunciar los delitos informáticos, dado que no se consideraba como un delito y por cuanto no había alternativas para denunciar estas acciones ilícitas. Si bien el sujeto activo no tiene un modus operandi establecido, al ser este un delito computacional, el delincuente lo

ejecuta en tan solo unos minutos y de manera fácil borra algún tipo de rastro o evidencia, haciendo dificultosa la identificación del delincuente.

4.2.6.1.2. Sujeto activo.

El sujeto activo se conoce a quien, comete el hecho delictivo o cuya conducta infringe la ley y se adecua a un tipo penal. Es importante que mencionemos como considera a estos sujetos el sociólogo Sutherland quien los expresa como delito de “cuello blanco” (Shutherland, 1939) en su discurso ante la Asociación Americana de Sociología donde además señala que “un crimen cometido por una persona de respetabilidad y de alto estatus social en el curso de su ocupación” (Shutherland, 1939, pág 1.) Otorgando así la explicación que no puede ser cualquier persona el sujeto activo de este delito; sino que requiere que este sujeto tenga cierta preparación técnica, habilidades en sistemas informáticos, conocimientos de los sectores estratégicos para una fácil vulneración. En definitiva, este perfil puede ser desarrollado por técnicos o profesionales en sistemas informáticos lo cual notoriamente hace que se diferencien de un delincuente común.

A este sujeto activo de los delitos informáticos se lo conoce o nombra como delincuente informático o cibercriminal tiene muchas denominaciones siendo las más técnicas las siguientes:

Hacker: es la persona que posee la experticia en todo lo referente a el manejo de sistemas quien puede acceder a los mismos sin autorización alguna con la única finalidad de sustraer información y de ocasionar daños en dichos sistemas. En la red de internet se lo define como “es una persona que entra de forma no autorizada a computadoras y redes de computadoras. Su motivación varía de acuerdo a su

ideología: fines de lucro, como una forma de protesta o simplemente por la satisfacción de lograrlo” (Castro, 2015).

Cracker: a diferencia del anterior crea y modifica software y hardware de computadoras, para desarrollar funciones o modificaciones.

Los hackers y crackers son individuos de la Sociedad moderna que poseen conocimientos avanzados en el área tecnológica e informática, pero la diferencia básica entre ellos es que los hackers solamente construyen cosas para el bien y los crackers destruyen, y cuando crean algo es únicamente para fines personales” (Castro, 2015).

Los crackers principalmente tienen la misión de desarmar programas para llegar a la protección de seguridad de los sistemas operativos y producir daños ahí.

Phreaker: esta persona es quien investiga los sistemas telefónicos mediante el uso de aparatos tecnológicos cuya finalidad varía, puede ir desde utilizar el servicio sin pagarlo hasta la reproducción fraudulenta de tarjetas prepago para llamadas telefónicas.

Virucker: Un virucker se dedica a la programación de virus informáticos, para con ellos producir daño al sujeto pasivo ya sea una persona natural o una persona jurídica o para difundir ideas radicales a manera de protesta.

Pirata informático: es aquel individuo que reproduce y distribuye a título gratuito u oneroso un software sin permisos legales del autor infringiendo los derechos de autor a cambio de que los usuarios suban o carguen a la página otros programas.

4.2.6.1.3. Bien Jurídico Protegido

En otros delitos el bien jurídico protegido suele ser la vida, la libertad, entre otros en este delito el bien jurídico al que hay que referirse es la información que es

susceptible a ser almacenada, tratada y transmitida a través de sistemas informáticos. Es de reconocer que la información en algunos casos llega a tener un gran valor económico para el titular de la misma.

Muchas empresas tienen su acervo informático que sirve para la gestión administrativa o para la toma de decisiones; esta información en manos de un delincuente informático puede ser utilizada para beneficio propio o para ser destruida o alterada ocasionando pérdidas a gran escala a dichas empresas. De igual manera, hay la información puede ser de índole personal, así lo establece la Dra. Zambrano:

Al cometimiento de un delito informático se viola lo que es más privativo de un ser humano como son los bienes intangibles amparados por el Derecho de Propiedad al manipularse sus datos personales y privados considerando que desde un nombre de dominio, una creación intelectual de cualquier índole, intimidad personal, dirección virtual o convencional, cometimiento de fraude, conlleva la seguridad jurídica en la red. (Zambrano, 2012)

Es de resaltar que los delitos informáticos pueden perjudicar al buen nombre, al honor a derechos que la ley garantiza a la persona, la información como bien jurídico tutelado también engloba:

- La reserva, la intimidad y confidencialidad de los datos
- La seguridad o fiabilidad del tráfico jurídico y probatorio
- El patrimonio

4.2.6. Elementos para que se configure el delito de estafa informática

Con todas las definiciones existentes de estafa informática y los perjuicios que esta ha causado países como España, Alemania, Francia, Suiza y Norteamérica en sus ordenamientos jurídicos ya han regulado a la estafa informática mediante el uso de

datos o mediante la alteración o introducción de programas orientados a solucionar los injustos causados por desarrollos informáticos.

En la doctrina acerca de la criminalización de la estafa informática y la relevancia de esta, con la estafa común se puntualiza que:

Del fraude o estafa informática viene a colmar una laguna legal derivada de la inadecuación del tipo de estafa para hacer frente a determinados ataques al patrimonio mediante la alteración o manipulación de datos informatizados. El concepto general de estafa introducido por la reforma de 1983 suponía la exigencia de un engaño capaz de producir error en otra persona, de forma que provocará un acto de disposición sobre su propio patrimonio o el de un tercero. La dinámica comisiva no podía soslayar la existencia del error sobre la disposición patrimonial, son pena de renunciar a la relación de causalidad e imputación objetiva del resultado lesivo a acción engañosa.

El enriquecimiento ilícito a través de la alteración de asientos contables u otros datos informatizados con relevancia económica en el patrimonio ajeno, tan sólo podía encontrar respuesta penal en la estafa mediante una hermenéutica voluntarista. En definitiva, la criminalización de las manipulaciones informáticas tendentes a provocar la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero debe considerarse un acierto. (Muñoz V. , pág. 490).

Se habla de que el tipo común de estafa no es el adecuado para enmarcar la estafa informática si bien, en ambos se produce un daño al patrimonio de un sujeto en este último tipo de estafa informática se emplean otros mecanismos e incluso en este se pueden producir daños o pérdidas económicas a una escala mayor por la información

que el sujeto activo de este delito puede llegar a tener alcance y el uso que de los mismos.

Para qué exista el delito de estafa informática debe cumplir con los requisitos siguientes:

Obtener un resultado. - No necesariamente el resultado del acto debe ser falso, porque se puede obtener un resultado verdadero sin embargo lo podemos reemplazar por otros datos, estos casos son comunes en los delitos de estafa informática en donde se obtiene un beneficio económico.

Datos. - Deberá tratarse de actos que manejen datos para lesionar el patrimonio del titular de los datos o de terceros, o a su vez, si se utiliza datos falsos. Los casos más comunes son en los delitos de phishing. De tal manera deberá realizarse la introducción, alteración, borrado o supresión de datos;

Tecnologías de la Información y la Comunicación. - El acto debe realizarse a través del uso de las Tecnologías de la Información y Comunicación, el mismo que deberá ser contado como inicio, medio y final;

Lucro. - Es importante señalar que en un delito de estafa siempre existirá un lucro, puesto que el delincuente busca ganancias pecuniarias, en la estafa informática, debe necesariamente existir un lucro, puesto que, al no existir dicho tipo penal, y al no configurarse estaríamos hablando de sabotaje informático o acceso ilícito; y,

Bien jurídico. - Como preámbulo del bien jurídico protegido es necesario identificar de qué se trata y su importancia; para luego desarrollar cual es el bien jurídico protegido que lesionan el delito de estafa informática. Por ello se recurre a la doctrina en donde Von Liszt respecto a los bienes jurídicos en general menciona que son: “[...] intereses vitales, interés del individuo o de la comunidad. No es el

ordenamiento jurídico lo que genera el interés, sino la vida; pero la protección jurídica eleva el interés vital al bien jurídico. Los intereses vitales deben ser indispensables para la convivencia comunitaria luego de lo cual y como consecuencia de ello serán protegidos normativamente bajo juicios de valor positivo.” (Von. Liszt citado por Bustos, 1981, pág. 131).

Los bienes jurídicos en este caso en materia de Derecho Penal, representan los intereses colectivos de la Sociedad; los cuales tienen un valor relevante por lo mismo el legislador considerando imprescindible su protección a través de la norma Penal jurídicamente los enmarca en una protección y ante su vulneración impone una pena. Ya que el desarrollo de las ciencias informáticas y las Nuevas Tecnologías, han traído consigo delitos informáticos y en concreto el delito de estafa a través de medios informáticos.

Si bien en los delitos informáticos, la atención de los bienes jurídicos, se realiza desde la perspectiva de los delitos tradicionales, siendo así que reinterpretan los tipos penales que ya existen con la finalidad adaptarlos a los distintos tipos de delitos, como por ejemplo el fraude financiero. Es necesario que esta valoración del bien jurídico protegido en la estafa informática se realice con la introducción de valores inmateriales, siendo la información uno de estos bienes intangibles a ser protegidos. Es importante en este punto resaltar que efectivamente la información y otros bienes de carácter intangible son bienes que se encuentran protegidos constitucionalmente, aunque es de considerar que su valoración económica difiere de los bienes corporales.

“Los delitos informáticos tienen el carácter de pluriofensivos o complejos, es decir, que se caracterizan porque simultáneamente protegen varios intereses jurídicos, sin

perjuicio de que uno de tales bienes está independientemente tutelado por otro tipo. En conclusión, no se afecta un solo bien jurídico, sino una diversidad de ellos” (Magliona Markovicth, 1999, pág. 68).

De acuerdo con este criterio el bien jurídico protegido en este tipo de delitos que de los versa este trabajo de investigación, como ya se hizo mención en general es la información, pero esta debe ser considerada en diferentes formas:

1. como un valor económico,
2. como uno valor intrínseco de la persona, por su fluidez y tráfico jurídico,
3. por los sistemas que la procesan o automatizan;

Estas formas son de considerar que son los mismos que se equiparan a los bienes jurídicos protegidos tradicionales entre ellos:

- a. El patrimonio,
- b. La reserva, la intimidad y confidencialidad de los datos
- c. La seguridad o fiabilidad del tráfico jurídico y probatorio, en falsificaciones de datos o documentos vía medios informáticos.

4.2.6.1. Tipos de Estafa Informática

Es de relevante valor académico en el desarrollo del presente estudio, analizar los delitos informáticos más comunes que se desarrollan en los medios informáticos y que la mayoría de personas en ciertos casos se tiene un total desconocimiento del nombre y definición de estos tipos de estafa informática.

4.2.6.1.1. Phishing:

En términos simples se puede definir que hablamos del robo de la información de datos personales, a través de un correo electrónico que aparentemente proviene de una institución que comúnmente es bancaria o empresarial con la se mantiene alguna

relación o afiliación; obteniendo así datos como claves, nombres, número de cédula, números de cuentas bancarias, dirección o teléfono entre otros con falsos argumentos como transferencias o confirmación de actualizaciones e incluso la entrega de premios.

“El término phishing proviene de la unión de los siguientes vocablos en inglés password, harvesting y fishing, con lo que se viene a hacer alusión a “cosecha y pesca de contraseñas”. A la persona que pone en práctica este delito se le conoce como phisher.” (Caro, 2015). Hablamos del tipo de engaño que es realizado con la finalidad de robar la identidad del usuario, generalmente utilizado en el correo electrónico. Existen varias definiciones al respecto que buscan exponer en qué consiste este tipo de delito informático entre ellos es conveniente citar una de ellas:

Es un delito informático que, a través del uso de las Tecnologías de la Información y Comunicación, que, programando un sistema de comunicación confiable y legítimo, se obtiene información o datos de personas titulares o terceros, con la única finalidad de buscar un lucro. (Ron, 2019))

Mediante este método el ciber-delincuente tiene a su alcance datos como:

- Los números de su tarjeta de crédito o débito.
- Números de cédula o pasaportes.
- Claves secretas.
- Contraseñas.
- Coordenadas e-key.
- Direcciones.
- Teléfonos.

El phishing es uno de los métodos de fraude más comunes, y que busca engañar al usuario, generalmente haciéndole suministrar sus datos a través de una página falsa. Los datos posteriormente son utilizados por el estafador para distintos fines, tales como la venta de la información captada (el caso de nombre de usuarios, correos y redes sociales); la sustracción de fondos (cuando se obtienen contraseñas, datos de tarjeta de crédito o bancarios); o incluso el “secuestro” de las cuentas para pedir rescate a los usuarios. (Cueva, 2015).

El término Phishing según los tratadistas citados es un método utilizado por los delincuentes para conseguir información personal o contraseñas realizada a través de las tecnologías de la información y la comunicación ya puedan ser estas a través de correos electrónicos, mensajes de texto o mensajes en redes sociales mediante el cual la persona tras estos mensajes insertan enlaces de páginas previamente modificadas para que estas aparentemente parezcan originales ya sea de un banco, una empresa que ofrezca productos, empleo, o servicios de pagos, una vez que la posible víctima ha abierto este link la página falsa solicita que se ingrese datos personales, en caso de un banco la supuesta actualización de datos o incluso hasta contraseñas. Las formas de phishing más usuales son:

1. Mensajes Cortos (SMS): Se envían al sujeto usuario de algunas entidades mensajes, solicitando ciertos datos de carácter personal. Como por ejemplo notificando al usuario que es beneficiario de cierto concurso y que para reclamar el premio del mismo debe facilitar su información.
2. Llamadas Telefónicas: En este caso el usuario recibe una llamada telefónica en donde el sujeto activo de este delito suplanta a la identidad de un funcionario o empleado de entidad privada o pública solicitando datos personales.

3. Páginas Web: Es común para usuarios de esta red encontrarse con simulaciones de la página web oficial de la entidad requerida, o sitios web falsos con señuelos llamativos, en donde le piden al usuario que facilite datos personales con la única finalidad de ser mal utilizados o enviando correos basura al correo personal del usuario.

4.2.6.1.2. Smishing

Entre los peligros del internet se encuentra el smishing, esta consiste en una forma de phishing que busca la suplantación de identidad. En términos informáticos es una técnica de envío de mensajes de texto a teléfonos móviles, pasando a términos legales puedo referirme a este como un delito mediante el cual el mensaje de texto tiene la única finalidad de infectar el dispositivo del usuario para obtener claves u otra información personal o vender servicios falsos.

El término smishing se refiere al phishing, pero mediante SMS, que son los mensajes cortos que se pueden enviar entre teléfonos celulares; conocidos también como el servicio de mensajería instantánea. Este nuevo tipo de delito es realizado a base de técnicas de ingeniería social. El smishing es una amenaza emergente y en crecimiento en el mundo de la seguridad en línea.

Entre las definiciones más comunes de este tipo de estafa informática encontramos que es señalada como:

Un delito informático y una variante del phishing, que, a través de programas de mensaje de texto por medio de Tecnologías de la Información y Comunicación, que, programando un sistema de texto confiable y legítimo, se obtiene información o datos de personas titulares o terceros, con la única finalidad de buscar un lucro. (Ron, 2019)

El smishing en la obra Delitos y Delincuentes de varios autores del Club Universitario de Alicante dice que “consiste en recibir un SMS en el que se indica que hemos sido dados de alta en un determinado servicio y para poder dar de baja hay que llama a un número en el que nos solicitan nuestros datos para posteriormente utilizarlos con fines ilícitos” (2010, pág. 35).

Los mensajes empleados para el cometimiento de este delito son recibidos por la víctima con tono de urgencia instándolo a tomar acción. Es decir, con el Smishing se envía un mensaje de texto al teléfono del usuario, dicho mensaje de texto normalmente solicita al usuario llamar a un número de teléfono o ir a un sitio web. La llamada telefónica es respondida usualmente por un sistema de respuesta automatizado.

Las víctimas de smishing reciben mensajes **SMS** similares a estos:

- "Estamos confirmando que se ha dado de alta para un servicio de _____. Se le cobrará 2 dólares al día a menos que cancele su petición en la plataforma: www.....com."
- “Usted es beneficiario de un premio económico por la fidelidad a nuestra institución bancaria, gracias de llamarnos para completar las informaciones para hacer efectiva la entrega al número"”
- Se notifica que su cuenta bancaria ha sido bloqueada por transacciones no frecuentes para desbloquear la misma, favor de llamarnos para completar las informaciones al número
- Mensajes atractivos como “FELICIDADES, ha sido seleccionado de entre millones de usuarios con un [auto]. Para obtener su premio envía al [número] la

palabra “COCHE”, es muy común por parte de los ciberdelincuentes para estafar a sus víctimas con una suscripción a un servicio SMS premium.

En algunas ocasiones al visitar el sitio web que indica, las víctimas son forzadas a descargar algún tipo de programa que generalmente suele ser un virus troyano. Esta táctica se aprovecha de la confianza del usuario para obtener información.

Esta modalidad de estafa informática está dirigida a clientes o usuarios de compañías telefónicas a base de técnicas de ingeniería social, la diferencia de este tipo de estafa con el Phishing es que los ciberdelincuentes simplemente utilizan mensajes de texto o SMS en lugar de correos electrónicos. En definitiva, son factores que lo convierten en una amenaza para la seguridad, considerando que el uso actual de los teléfonos celulares ha llegado a ser indispensable; este delito se está convirtiendo en una amenaza empresarial, así como una amenaza a los consumidores de estos equipos y telefonías. Según el blog de seguridad más popular llamado CLOUDMARK ha señalado que el smishing se ha convertido en la principal forma de enviar mensajes maliciosos.

Este tipo de estafa se trata del uso del phishing-métodos de engaño para obtener información personal confidencial o estafar a alguien- pero a través de SMS (mensajes cortos de celular) en lugar de correos electrónicos, apareció en 2008, pero los expertos dicen que ha aumentado en los últimos años, no sólo a través de mensajes de texto sino también en aplicaciones de mensajería como WhatsApp. Este tipo de fraudes funcionan enviando mensajes que manipulan y tienden trampas a las víctimas para que hagan clic en enlaces fraudulentos. (Tecnología, 2017).

En conclusión, este es un anzuelo para obtener información personal, en el smishing los realizadores de este delito tienen varias estrategias de texto para llegar a las

víctimas en el caso que indican falsamente al usuario que se ha bloqueado su cuenta bancaria, solicitan así confirmación de número de cédula, de número de cuenta, contraseñas e incluso el código CVV de sus tarjetas de débito o crédito y ya una vez con estos datos podrían realizar compras en línea. El smishing es alarmante porque las personas tienden a confiar más en los mensajes de texto que en los mensajes de correo electrónico. La mayoría de las personas son conscientes del riesgo para la seguridad que conlleva hacer clic en vínculos incluidos en mensajes de correo electrónico. Sin embargo, no puede decirse lo mismo cuando se trata de mensajes de texto. Casi todos los mensajes de texto que se reciben a diario no representan ninguna amenaza, pero solo es necesario un mensaje malicioso para comprometer la seguridad de una persona.

4.2.6.1.3. Vishing

Vishing es una combinación de las palabras voz y phishing, dado que se refiere a una de las estafas de phishing, pero esta es ejecutada mediante vías telefónicas, este delito informático busca o intenta engañar para que se revele información de carácter financiero o personal. El vishing funciona igual que el phishing, pero no siempre es ejecutado mediante internet, se lleva a cabo por la tecnología de voz. Entre las definiciones por los expertos en las técnicas de ingeniería social se señala que:

Es un delito informático y una variante del phishing, que, a través de líneas telefónicas por medio de Tecnologías de la Información y Comunicación, que programando un sistema telefónico confiable y legítimo, se obtiene información o datos de personas titulares o terceros, con la única finalidad de buscar un lucro. (Ron, 2019)

Otra definición referente a este delito es la que da Fernández en el señala que este tiene un modo de operar similar al phishing además de explicar de dónde proviene la palabra vishing, este autor explica que “el vishing es una combinación de las palabras «voz» y “phishing”. Se refiere a estafas de phishing que se hacen por teléfono. A los individuos se les intenta engañar para que revelen información crucial de carácter financiero o personal. El vishing funciona igual que el phishing, pero no siempre ocurre por internet y se lleva a cabo mediante tecnología de voz” (Fernández, 2019).

En este delito de estafa informática opera debido a que logran orquestar factores que los hacen sonar legítimos de la siguiente manera:

1. Cuenta con información correcta: es decir que tienen su nombre, dirección, número telefónico e información bancaria aparentando tener toda la información que usted esperaría escuchar de un funcionario de verdad de una entidad bancaria.
2. Manifiestan urgencia: hacen creer que su dinero está en peligro, y que debe actuar con rapidez induciendo miedo, lo que suele llevar a las personas a actuar sin pensar.
3. Tienen habilidades telefónicas: el número de teléfono parece provenir de otro sitio (como ocurre con el spoofing). Así que contesta el teléfono con intención de creerle a quien le llama, dado que el número parece convincente.
4. Una aparente atmósfera empresarial: se escucha mucho ruido de fondo, de modo que da la impresión de ser un «call center».

Esta técnica de práctica criminal, opera con el objetivo principal de obtener toda la información posible de su víctima a través de los sistemas telefónicos automatizados

para establecer fraudes bancarios especialmente con tarjetas de crédito y códigos de acceso para transacciones en línea; logran realizar este tipo de actos dado que suplantan o roba la identidad de su víctima.

El vishing es un delito informático que se deriva del phishing, pero qué se diferencia de éste al no ofrecer un enlace (link) para que la víctima haga clic en él, sino que a través de un número de teléfono al cual comunicarse. Para llevar a cabo el vishing, los delincuentes hacen uso de sistemas de telefonía IP o voz automatizada. Se realizan llamadas aleatoriamente a algunos números, a la persona que contesta se le informa que su tarjeta de crédito o cuenta bancaria está siendo utilizada fraudulentamente y deberá llamar a un número específico de su entidad bancaria; o, también se le puede solicitar datos personales llamando a un número telefónico específico.

Si bien los ataques de vishing son difíciles de rastrear, dado que se usan tecnología de Voip que es voz sobre IP, lo que significa que en su mayoría las llamadas son desde un computador, cuya ubicación puede ser en cualquier parte del mundo. Para una mejor comprensión analicemos este tipo de estafa con un ejemplo:

1. El criminal configura su computador para llamar a números telefónicos en una determinada región.
2. Cuando la llamada es contestada, se reproduce una grabación en la cual alerta al usuario que hay inconvenientes con su cuenta bancaria y que este debe llamar al número que sigue inmediatamente. El número puede ser un número gratuito pero falso para la compañía financiera que se pretende representar.
3. Cuando la víctima llama a este número, es contestada por una voz manipulada por computadora o donde se finge la apariencia de ser un call center, que le indica al

"cliente" que su cuenta necesita ser verificada y le requiere que ingrese los dígitos de su número de cuenta.

4. Cuando la persona provee la información, el visher tiene toda la información necesaria para realizar cargos o transacciones de la cuenta de la víctima.
5. La llamada puede ser también utilizada para obtener detalles adicionales como el **PIN** de seguridad, la fecha de expiración, el número de cuenta u otra información importante.

Al acceder a cualquier tipo de servicio telefónico o de comunicaciones sobre Internet, los usuarios para salvaguardar su información confidencial; es esencial que no proporcionen información personal a través de llamadas telefónicas, deben asegurarse que es la persona o entidad que inicia una llamada y más importante aún es no dar información telefónica de números de tarjeta, cuentas bancarias, cédula de identidad, número de cédula.

En conclusión, el vishing es una vuelta de tuerca a la estafa, que combina teléfono e Internet. El 'vishing', junto al 'phishing' y al 'smishing' son algunas de las amenazas tecnológicas de estos tiempos.

4.2.7. Diferencias entre estafa y estafa informática

Dentro del desarrollo del presente estudio es necesario puntualizar las diferencias entre estafa convencional y estafa informática, con la finalidad de tener claro la adecuación al tipo penal de cada uno de estos dos delitos.

En cuanto a la estafa común el elemento central es el engaño o la conducta engañosa que debe ser la idónea para influir en otras personas para producir un error, exigiendo la presencia física del autor del delito de estafa se configura cuando el agente haciendo uso del engaño, astucia, ardid u otra fraudulencia induce o mantiene en

error al sujeto pasivo con la finalidad de hacer que éste en su perjuicio se desprenda de su patrimonio o parte de él y le entregue voluntariamente a aquel en su directo beneficio indebido o de un tercero. Juristas como Mata y Martín se pronuncian sobre este error al que se induce a la víctima señalando que es “tanto desde un prisma objetivo como subjetivo— para producir error a otra u otras personas” (2008, pág. R5:2).

Es así que los elementos típicos de la estafa se encuentran encadenados sucesivamente uno al anterior; produciendo así una reacción causal en cadena, siendo cada elemento considerado consecuencia del anterior y causa del posterior. “Sin embargo, esta tradicional vinculación a la dimensión causal del engaño, en el sentido de su eficacia naturalística para producir el error, ha dado paso a otros criterios objetivos, como la moderna teoría de la imputación objetiva, que amplía los factores determinantes de la tipicidad de la estafa” (Mata & Martín, 2008, pág. R5: 3).

En cambio, en cuanto a la estafa informática implica el empleo fraudulento de medios electrónicos que no necesariamente requiere de la presencia física de la víctima con al menos un contacto personal es suficiente para ejecutar la acción además la estafa informática es la introducción, alteración, borrado o supresión indebida de datos informáticos, especialmente datos de identidad, y la interferencia ilegítima en el funcionamiento de un programa o sistema informática.

Mata & Martín explican que “El elemento determinante de la nueva modalidad defraudatoria y que además permite filtrar los supuestos correspondientes a la estafa convencional, es la existencia de una manipulación informática” (Mata & Martín, 2008, pág. R5: 6).

Dado el carácter de la fórmula empleada se han suscitado dos interpretaciones tanto doctrinal y jurisprudencialmente, que destaca la consecuencia última de la alteración del resultado del procesamiento automatizado y no tanto la forma de la acción realizada. De tal forma que por manipulación habría de entenderse cualquier alteración del resultado de un procesamiento electrónico de datos. Se entiende por otra forma que no se atiende tanto a las consecuencias sino al objeto sobre el que se pretende o actúa el sujeto activo descartando la intervención sobre los datos y sobre el hardware e incluyendo únicamente las actuaciones manipulativas sobre las instrucciones de procesamiento automatizado del sistema informático (software).

En conclusión, la diferencia entre el delito de estafa convencional y el delito de estafa informática, es la forma operativa que en la primera se requiere la presencia física del sujeto activo y en la segunda no, además la estafa convencional es el engaño o la conducta engañosa y en cambio la estafa informática es la introducción, alteración, borrado o supresión indebida de datos informáticos. Por lado en la estafa informática solo es necesario el uso de medios electrónicos y las consecuencias que se desencadenan, destacando que el primer tipo de estafa el objetivo es un bien patrimonial actividad realizada mediante en contacto personal, es decir, cara a cara entre el sujeto pasivo y sujeto activo, mientras que en el segundo es la obtención de la información a través de medios o dispositivos electrónicos sin necesidad de que exista un contacto directo entre sujeto pasivo y sujeto activo para posteriormente producir una afectación patrimonial.

4.3. MARCO JURÍDICO

4.3.1 La Protección al Derecho a la Propiedad en la Constitución de la República del Ecuador

La presente investigación está enmarcada y fundamentada en la Constitución de la República del Ecuador- como norma suprema dentro de nuestro ordenamiento jurídico interno prevalece sobre otras normas y tratados internacionales, por lo que es necesario ir analizando los siguientes Artículos:

Artículo 26 de la Constitución de la República; en cual se reconoce y garantiza a las personas “El Derecho a la propiedad en todas sus formas, con función y responsabilidad social y ambiental. El Derecho al acceso a la propiedad se hará efectivo con la adopción de políticas públicas, entre otras medidas” (CRE, RO 449:2008).

De este artículo puedo manifestar que nuestra Constitución protege el Derecho a la propiedad de todas las personas sin distinción alguna, reconoce a la propiedad como un Derecho que versa sobre el poder legal e inmediato que tiene una persona para gozar, disponer y reivindicar sobre un objeto o propiedad, sin afectar los derechos de los demás ni sobrepasar los límites impuestos por la ley, siendo más precautelada la propiedad privada por las normas de protección que dicta la misma Constitución. Con este Artículo el Estado busca cumplir un rol activo en la función social de la propiedad para facultar la organización de la economía.

En el Artículo 321 la Constitución de la República como complemento del Artículo anterior se enmarca que “El Estado reconoce y garantiza el Derecho a la propiedad en sus formas pública, privada, comunitaria, estatal, asociativa, cooperativa, mixta, y que deberá cumplir su función social y ambiental” (CRE, RO 449:2018).

Es así que el presente Artículo definitivamente se constituye en una extensión del anterior, ratificando el principio general del reconocimiento de derechos fundamentales siendo estos por derivación de la naturaleza de la persona y por su adecuación al bien de la misma manifestación de la autonomía individual como miembros de la Sociedad. Por otra parte, este Derecho que implica para el propietario la facultad plena, omnímoda, de usar, gozar y disponer de la cosa, y; al mismo tiempo, el poder de no usar, de no gozar, de no disponer de la cosa misma. Con este Artículo se busca incluso, regular nuevos institutos fuera de lo que tradicionalmente se concibe como forma de propiedad todos en torno a que propiedad es el poseer alguna cierta cosa y poder disponer de ella dentro de los límites legales.

4.3.2. Estafa Informática en Leyes y tratados Internacionales

4.3.2.1. Convenio sobre Ciberdelincuencia

Celebrado en Budapest el 23 de noviembre del 2001, para proteger a la Sociedad frente a la ciberdelincuencia, por los cambios provocados por la digitalización, la convergencia y la globalización continua de las Tecnologías de la Información y la Comunicación y la información que éstas contienen, ponen en riesgo a la Sociedad en general de ser víctimas de delitos informáticos entre estos el delito de estafa informática, en su Artículo 8 establece que los estados partes deberán “tipificar como delito en su Derecho interno los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante: a.- cualquier introducción, alteración, borrado o supresión de datos informáticos; b.- cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona” (Europa, 2001).

Dado que, si bien nuestro país no figura como uno de los países que ratifican dicho convenio, es conveniente resaltar el objetivo del mismo, considerando que los modelos internacionales son bastos en nuevas concepciones legislativas, por lo tanto, son un punto de referencia legislativa. Este convenio busca hacer frente a los **delitos informáticos, entre ellos a la estafa informática** y los delitos cometidos a través del **Internet** mediante la **armonización de leyes** entre naciones, para que cada estado parte tome las respectivas medidas para contrarrestar la ciberdelincuencia. Es por eso que para mejorar las técnicas de investigación e implementar delitos como es la estafa informática y sus variaciones en nuestro ordenamiento jurídico; nuestro Estado debería formar parte de este convenio de ciberdelincuencia y de esta manera adaptar nuestra legislación penal a este convenio con la finalidad de brindar protección a la Sociedad contra el cibercrimen fomentando así la cooperación internacional para combatir delitos informáticos.

Este convenio tiene tres ejes sobre los cuales se desarrolla, respecto al primero en torno a establecer un catálogo de figuras de delitos informáticos y a penar estas modalidades de criminalidad. El segundo eje arma normas procesales sobre los cuales se busca mantener herramientas procesales contra la manipulación de evidencia informática o en formato electrónico y a los delitos cometidos con la utilización de un medio informático. Y finalmente el otro eje que contiene son las normas de cooperación internacional, estas son disposiciones sobre la localización de sospechosos, recolección o envío de evidencia digital e incluso se hace referencia a la extradición. Es así que con este convenio de ciberdelincuencia se logra tipificar conductas de delitos informáticos en todos los países, además unificando normas

procesales de cualquier delito que existan evidencia digital se busca una cooperación internacional.

El que nuestro país se sume a este convenio significaría un gran adelanto en materia de investigación de delitos informáticos, además de ello este convenio nos aportaría herramientas y procedimientos que actualmente son necesarios para en nuestro país pueda luchar con el cibercrimen. Una herramienta que vale destacar de este convenio es la que define el Artículo 35, del convenio cual propone la designación de un punto de contacto para la red 24x7 que es para proveer apoyo y cooperación de forma rápida. Por todas estas razones expuestas es que resulta muy conveniente que nuestro país se adhiera a este convenio y es aún más necesario el que actualice su catálogo de delitos introduciendo los delitos informáticos, en especial la estafa informática que es uno de los delitos informáticos más comunes en nuestro país.

4.3.3. El Delito de Estafa en Código Orgánico Integral Penal (COIP)

El Código Orgánico Integral Penal cumple un papel muy importante dentro del marco jurídico de la presente investigación, por ello es relevante iniciar estas referencias con lo establecido en su Artículo 2 que versa sobre principios generales afines al debido proceso: “En materia penal se aplican todos los principios que emanan de la Constitución de la República, de los instrumentos internacionales de derechos humanos y los desarrollados en este Código” (COIP, RO 180;2014).

Considerando que los principios son las garantías fundamentales para la organización jurídica de un estado como el nuestro, debemos concebirlos como la forma en que se consolida en límite a la actividad de los operadores de justicia, dado que tiene la potestad de impedir cualquier actuación contraria al ordenamiento jurídico vigente.

Ya en relación con nuestro tema y problema planteado, es merecedor que para tratar delitos informáticos en nuestro Código Orgánico Integral Penal sean estos, siguiendo los principios procesales que emana la Constitución y los Tratados Internacionales a los cuales como país nos encontramos suscritos.

En cuanto a los principios el Código Orgánico Integral Penal se encuentra regido por veintiún principios fundamentales para un debido proceso penal comprendidos en el Artículo 5 de los cuales considero que es conveniente hacer mención dentro de esta investigación al inciso 1, referente al principio de legalidad en el que se establece:

1. “Legalidad: no hay infracción penal, pena, ni proceso penal sin ley anterior al hecho. Este principio rige incluso cuando la ley penal se remita a otras normas o disposiciones legales para integrarla” (COIP, RO180;2014).

Este principio conforme lo estipula la legislación penal vigente de nuestro país, cuya esencia es: *nullum crimen nulla poena sine previa lege* (no hay delito ni pena sin ley previa). Por cuanto, si una acción no está señalada en la ley como un delito, no puede ser considerado como tal; y por ende no existe una sanción por el mismo. En cuanto a la injerencia del principio de legalidad con los delitos informáticos, es de destacar que la estafa informática y sus modalidades que entre los más comunes son phishing, smishing y el vishing; son delitos que no constan en la legislación por cuanto no puede ser objeto de sanción alguna, permitiendo que se den una gama de perjuicios al patrimonio de los ciudadanos.

En cuanto al Artículo 186 el delito de Estafa común de la siguiente forma: “La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que

perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años” (COIP, RO 180;2014).

En la definición del delito de estafa se encuentran los elementos: engaño, error, acto de disposición patrimonial, perjuicio y ánimo de lucro a los que debemos añadir el nexo causal y demás exigencias típicas de la imputación objetiva. Este Artículo de la ley mencionada establece las sanciones describiendo las situaciones en las que se incurre en el delito de estafa, específicamente el numeral que corresponde al análisis al tema a desarrollar es el numeral 2 que establece:

“La pena máxima se aplicará a la persona que: 2. Defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares” (COIP, RO 180;2014).

En este sentido el Código Orgánico Integral Penal, no se encuentra tipificando el delito de estafa informática concretamente dado que comúnmente los operadores de justicia confunden el delito de estafa informática con el numeral 2 de este Artículo ya que el mismo hace referencia al uso de dispositivos electrónicos para cometer este delito con una limitante muy clara al momento de referirse específicamente a la alteración, modificación, clonación o duplicación de dispositivos de un cajero automático con la finalidad de robar información no consentida de tarjetas de débito, crédito, pago similares, pues cabe recalcar que la información personal no solamente se la puede adquirir por medio de un cajero automático sino que también por medio del uso de computadoras, teléfono móvil, redes sociales, correos electrónicos sin la necesidad de la presencia física del sujeto activo de este tipo de delitos.

Al existir este limitante de no encontrarse tipificado el delito de estafa informática, se da espacio a que exista una mala interpretación del mismo, además con el error de conceptualización en la legislación penal el operador de justicia no puede juzgar adecuadamente. Considerando además que el principio de legalidad juega un papel muy importante como se ya se hizo mención anteriormente, dado que no se considera delito a una acción no tipificada y por ende no puede existir sanción alguna. Es así que queda abierta la posibilidad del cometimiento de delitos informáticos en específico la estafa informática este tipo de cibercrimen que día a día evoluciona con los avances de la tecnología y buscan causar un perjuicio a un tercero mediante la manipulación informática consiguiendo transferencias patrimoniales no consentidas por su titular.

Es conveniente analizar también el Artículo 13, del Código Orgánico Integral Penal sobre las normas de interpretación: Las normas de este Código deberán interpretarse de conformidad con las siguientes reglas: “1. La interpretación en materia penal se realizará en el sentido que más se ajuste a la Constitución de la República de manera integral y a los instrumentos internacionales de derechos humanos. 2. Los tipos penales y las penas se interpretarán en forma estricta, esto es, respetando el sentido literal de la norma. 3. Queda prohibida la utilización de la analogía para crear infracciones penales, ampliar los límites de los presupuestos legales que permiten la aplicación de una sanción o medida cautelar o para establecer excepciones o restricciones de derechos” (COIP, RO 180;2014).

El presente Artículo nos lleva a concluir que, dado que no hay una norma específica para los delitos informáticos y que según lo establecido en el Artículo 186, en el que define a la estafa, sus penas según las condiciones efectuadas y que pretende hacer

calzar el delito de estafa informática, pero que jurídicamente resulta ser insuficiente; no puede ser interpretado o considerado como una analogía de lo que en realidad son los delitos informáticos y su alcance, quedando así la legislación penal insuficiente frente a este tipo de delitos. Con estas referencias es de señalar que al no cumplir con lo establecido en el Artículo 13 del Código Orgánico Integral Penal, se estaría contraponiendo al Artículo 82 de la Constitución de la República que señala:

“El Derecho a la seguridad jurídica se fundamenta en el respeto a la Constitución y en la existencia de normas jurídicas previas, claras, públicas y aplicadas por las autoridades competentes” (CRE, RO 449:2008)

Dado que, en la realidad Penal jurídica de nuestro país, al no existir una legislación penal adecuada a la continua evolución de la Sociedad con los avances de la tecnología no está brindando una seguridad jurídica a los gobernados, ni por las normas, ni por las Autoridades que las aplican dado que pone en tela de duda y evidencia que no se da una correcta administración de justicia.

Además, es de señalar que el Artículo 75, de la Constitución de la República del Ecuador, manifiesta que: “Toda persona tiene Derecho al acceso gratuito a la justicia y a la tutela efectiva, imparcial y expedita de sus derechos e intereses, con sujeción a los principios de inmediación y celeridad; en ningún caso quedará en indefensión. El incumplimiento de las resoluciones judiciales será sancionado por la ley” (CRE, RO 449:2008).

En cuanto a la estafa informática no se estaría cumpliendo con los derechos de protección dado que el Estado deber proveerse jurídicamente para la nuevas formas delincuenciales y brindar la protección y seguridad que les debe a los ciudadanos; considerando que no se podría hacer uso de las garantías de acceso gratuito a la

justicia y a la tutela efectiva, imparcial y expedita de sus derechos e intereses, con sujeción a los principios de inmediación y celeridad, por encontrarse actualmente el delito de estafa informática y sus modalidades más comunes phishing, vishing y smishing como delito inexistente en la legislación penal de manera detallada dentro del catálogo de delitos del Código Orgánico Integral Penal y que producen grandes perjuicios al patrimonio de la ciudadanía.

Ya que, en el desarrollo de la investigación he mencionado que uno de los bienes jurídicos que afecta el delito de estafa informática en sus diferentes modalidades son los datos de cada individuo dado que al acceder a ellos son puente para perjudicar al patrimonio, es conveniente ir hilando y aclarando ciertos aspectos jurídicos, como el Artículo 230 de la legislación penal en la que señala:

Interceptación ilegal de datos. - Será sancionada con pena privativa de libertad de tres a cinco años:

1. La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.
2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.

3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.

4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior. (COIP, RO 180;2014)

Este Artículo, hace alusión a los casos de robo de datos, acción que se produce cuando el sujeto pasivo se encuentra realizando un uso de redes sociales (sujeto activo usa datos de otra persona para hacerse pasar por alguien más y actuar de manera inescrupulosa ya sea inferir calumnias e insultos), uso de banca móvil al realizar un pago de alguna compra, con los datos del usuario y sin que este tenga conocimiento de ello, el más común es a través de la introducción o manipulación de programas o caballos de Troya y la técnica de salami que son programas destructivos escondidos, su ejecución genera un daño al sistema del computador aunque parezca que se está ejecutando una función normal en un computador o dispositivo electrónico, en realidad se está insertando instrucciones para efectuar una función no autorizada.

Si bien es cierto, este tipo penal guarda estrecha relación con el delito de estafa informática, que considero necesario tipificar dentro del Código Orgánico Integral Penal, en razón del cumplimiento del Artículo 13 del mismo cuerpo legal, en las normas de interpretación de la ley penal; que estipulan que la ley deberá ser interpretada en su sentido literal, es decir, que no hay lugar a suposiciones, sino que se la aplicara de conformidad a lo establecido y lo referente a la prohibición de la

utilización de analogías para crear infracciones penales o ampliar los presupuestos legales para aplicar sanciones.

Al implementar la estafa informática con elementos del tipo penal propio de la infracción, como lo han hecho países europeos como España o Alemania, se facilitaría el trabajo de los operadores de justicia, ya que al tener que sancionar una acción de esta índole, no tendrán que buscar adecuar dicha acción al tipo penal que más se adapte y de esta forma contravenir lo que estipula el art. 13 que hago mención, a la vez considero que se ahorraría recursos procesales.

Referente al Artículo 231 sobre las transferencias electrónicas de activos patrimoniales, la normativa penal estipula que:

La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona. (COIP, RO 180;2014)

Este tipo de actividad ilícita que hace mención el citado Artículo, comúnmente es realizada a través de la inserción de un virus el mismo que altera el funcionamiento de una computadora sin el permiso de su dueño, se propaga a través del software que al ser ejecutado ataca directamente al sistema operativo para el cual fue desarrollado, causando daños en los datos o destruyendo información del dispositivo alterando

completamente el funcionamiento y de esta forma logrando que el sistema operativo seleccionado proporcione información confidencial y personal.

Pero al igual que el artículo 230 guarda cierta relación con el delito que se pretende tipificar, pero la diferencia radica en que este tipo de acción se la realiza a través de la inserción de virus que en este caso altera el funcionamiento de un sistema operativo, la mayoría de los casos son ataques dirigidos a los usuarios de los servicios bancarios electrónicos, para acceder a cuentas e información personal y confidencial, para posteriormente apropiarse de su dinero.

Además es pertinente denotar que este artículo da lugar a una interpretación muy generalizada ya que no delimita el daño y activo patrimonial al que hace referencia, de esta manera, al juzgar una actividad o acción ilícita propia de la estafa, se estaría contraviniendo al Artículo 13 del mismo cuerpo legal ya que su redacción no es concreta y clara para mi criterio, por tal razón es que considero pertinente incluir al catálogo de delitos de Código Orgánico Integral Penal una disposición legal específica a las acciones cometidas por medio de las Tecnologías de la Información y la Comunicación y de su avance tecnológico, para evitar se queden en la impunidad.

Finalmente, referente a lo que dice el Artículo 232 sobre los ataques a los sistemas informáticos se regula que:

La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este Artículo.

2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.

Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad. (COIP, RO 180;2014)

Si bien podemos relacionar este Artículo con la estafa informática podemos enlazarlo a la parte operativa, específicamente a provocar daños a un Software y todo lo allí almacenado, es decir, al antes de la estafa informática y sus modalidades, dado que abarca la elaboración o distribución de programas maliciosos, pero no se refiere al daño patrimonial o al perjuicio económico que resulta de uso de estos programas, a mi juicio lo considero una agravante, a la tipología que ha sido objeto de estudio.

4.3.4 De la extraterritorialidad de los delitos

Referente a la extraterritorialidad contenida en el Código Orgánico Integral Penal, Artículo 404, numeral 6 este señala que:

Cuando la infracción se comete en territorio extranjero, la persona procesada será juzgada por la o el juzgador de la circunscripción territorial en la que es aprehendida o detenida o por la o el juzgador de la capital de la República del Ecuador. (COIP, Registro Oficial 180;2014)

Esto hace que ciertas personas responsables de delitos informáticos que se encuentren fuera del país, puedan ser sometidos a un proceso penal, pero no hay que

dejar de lado que se tendría cooperación internacional, aspecto importante en estos casos, ya que actualmente nuestro país no cuenta con dicha cooperación en casos de delitos informáticos, si no que únicamente en casos de delitos que atentan contra la integridad sexual o trata de personas; es por eso que considero que como país debería formar parte de convenios y tratados internacionales realizados para prevenir y erradicar la ciber delincuencia como el convenio celebrado en Budapest.

4.3.5 Tipificación del delito de Estafa Informática en el Derecho Comparado

4.3.5.1 La Estafa Informática en el Código Penal Español

En su Sección 1ª De las estafas, Artículo 248. Establece que cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno. También se consideran reos de estafa:

- a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.
- b) Los que fabricaren, introdujeran, poseyeran o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este Artículo.

Desde hace unos años esta legislación internacional contiene un apartado específico para la delincuencia informática, así que es posible ver la evolución que este tipo de delitos se va produciendo en España, permitiendo de esta forma a los operadores de justicia juzgar e imponer una sanción de manera correcta si bien es cierto el Código Penal Español no estipula un Artículo específico para el delito de estafa informática pero lo incluye dentro del delito de estafa común con un numeral específico para que no exista una laguna jurídica al juzgar delitos cometidos a través del uso de las

tecnologías de la información y la comunicación y a la vez estos no queden en la impunidad al no acoplarse a ninguna otra descripción del tipo penal cometido, cosa que sucede en nuestra legislación penal al tener tipificada la estafa común en el que únicamente incluye un tipo de delito informático cometido a través de cajeros bancarios limitando de esta forma a los operadores de justicia al juzgamiento de la estafa informática y sus modalidades de manera adecuada al no acoplarse a ningún tipo penal descrito en el Código Orgánico Integral Penal.

4.3.5.2 Estafa Informática en el Código Penal de Alemania

En su Artículo 263a. establece el delito de Estafa por computador en los siguientes términos; (1) Quien con el propósito, de procurarse para sí o para un tercero una ventaja patrimonial antijurídica, en la medida en que él perjudique el patrimonio de otro, por una estructuración incorrecta del programa, por la utilización de datos incorrectos o incompletos, por el empleo no autorizado de datos, o de otra manera por medio de la influencia no autorizada en el desarrollo del proceso, será castigado con pena privativa de la libertad hasta cinco años o con multa. (Republica Federal de Alemania, 1998).

Alemania tiene una ley adoptada contra la cibercriminalidad, contemplando específicamente la tipificación del delito de estafa por computador o también llamada estafa informática doctrinariamente, delito que es sancionado hasta con 5 años de privación de libertad en cambio en la legislación penal de nuestro país mantiene un vacío de tipo en la estafa informática si bien con el Código Integral Penal que entró en vigencia en el 2014 se buscó de cierta manera contemplar ciertos delitos informáticos pero en cuanto a la estafa informática seguimos frente a una legislación penal insuficiente. Considerando el modelo de tipificación alemán nuestra legislación

penal debería ser reformada y actualizada a el delito de estafa informática y sus modalidades: phishing, smishing, vishing para contar con la certeza de que estos delitos reciban una sanción correspondiente.

5. MATERIALES, TÉCNICAS Y METODOS

Para el desarrollo del presente trabajo investigativo utilicé distintos métodos, procedimientos y técnicas que me permitieron descubrir, sistematizar, ampliar conocimientos para poder dar posibles soluciones a la problemática planteada, mediante la reflexión comprensiva y el contacto directo con la realidad objetiva.

5.1. Materiales

5.1.1. Materiales de Oficina

Para dar cumplimiento a los objetivos propuestos de la presente investigación los materiales que utilice durante su desarrollo fueron:

- Equipos electrónicos: Tales como computadora de mesa y portátil, impresora, celular, grabadora de voz.
- Suministros de oficina: Papel bon A4, esfero gráfico. Lápiz.
- Redes y programas informáticos: El internet que fue una fuente guía para mi investigación, programa de Excel para elaborar los gráficos de la encuesta y entrevista y principalmente el uso de Microsoft Word.

5.1.2. Materiales bibliográficos

La recolección de material bibliográfico y de datos la realice a través de la técnica del fichaje para de esta forma manejar de mejor forma la presentación y también hice usos de la técnica del archivo por cuanto necesite del internet, páginas web

relacionados a mi tema de investigación, libros digitales, libros físicos, revistas jurídicas e informáticas, enciclopedias físicas y digitales, tesis de universidades nacionales e internacionales por lo que fue necesario recopilar y clasificar la información de acuerdo a su contenido e importancia.

También tome en consideración estudios jurídicos, normas jurídicas como la Constitución de la República del Ecuador, Código Orgánico Integral Penal, Convenios Internacionales y leyes penales de países como Alemania y España, a través del uso de la página jurídica LEXIS y VLex.

5.2. Técnicas

Para la elaboración de la parte teórica me apoye principalmente del fichaje y de archivo, que consistió en la elaboración de fichas bibliográficas y nemotécnicas las mismas que me permitieron recopilar la parte teórica del presente trabajo de investigativo. Además, utilice técnicas como:

5.2.1. La Encuesta

La técnica de la encuesta me sirvió para realizar investigación de campo y obtener información subjetiva sobre el tema investigado, la misma que fue aplicada de manera directa, es decir, acudí tanto a consultorios jurídicos particulares como públicos. La encuesta realizada fue aplicada a treinta profesionales del Derecho de la ciudad de Loja y Zamora, mediante un cuestionario de cinco preguntas relacionadas con los objetivos planteados dentro de la investigación.

La información recolectada contribuyó a reunir datos y conocer la opinión de cada encuestado sobre la problemática planteada, y la necesidad de incorporar un tipo

penal autónomo para la Estafa Informática y sus modalidades como consecuencia del desarrollo tecnológico para que sea juzgado con sus propias características.

5.2.2. La Entrevista

La entrevista al igual que la encuesta, consistió en la elaboración de cinco preguntas muy puntuales referentes al tema investigado, el mismo que lo apliqué personalmente mediante un dialogo con el entrevistado, la misma que la realice a juristas especializados y conocedores del tema y de la rama penal, de la ciudad de Loja.

Los criterios y sugerencias de los profesionales requeridos, sustentan la importancia y trascendencia jurídica y social del tema planteado, y la necesidad de proponer y dar solución a la problemática.

5.3. Métodos

En el desarrollo del presente trabajo de investigación utilicé el método científico que ha sido el instrumento más adecuado que me permitió llegar al conocimiento desarrollo, ejecución y dar posibles soluciones a la problemática planteada, mediante la reflexión comprensiva y el contacto directo con la realidad objetiva, es por ello que en la presente investigación hice uso de algunos métodos como:

5.3.1. Método Inductivo

Este método lo utilice desde la recolección de información referente al tema, partiendo de principios particulares, es decir, partiendo de temas o situaciones individuales, que partieron desde el problema y tema planteado en la investigación, la misma que me permitió descubrir temas generalizados requeridos dentro de la

presente investigación y que son de vital importancia para entender la problemática y la necesidad de hacer efectiva cada objetivo planteado.

5.3.2. Método Deductivo

Este método me permitió realizar un análisis partiendo desde el tema propuesto, descomponiéndolo en categorías principales para desarrollarlas en la investigación, hasta llegar a concluir en la situación específica del tema propuesto, este método me sirvió para deducir un camino a tomar y de esta forma proponer una solución al tema investigado, es decir, realice un análisis partiendo desde un tema general a un tema específico de la investigación propuesta. En este caso el de la necesidad de tipificar el delito de estafa informática y sus modalidades dentro de nuestro Código Orgánico Integral Penal, por las consecuencias y pérdidas patrimoniales que causa este delito.

5.3.3. Método Analítico

Este método me permitió al igual que el método deductivo desmembrar temas generales en sus partes o elementos que conforman la totalidad de la investigación propuesta de forma separada para observar las causas, la naturaleza y los efectos, establecer o generar analogías y nuevas teorías para de esta forma tener una mejor claridad del objeto de estudio y lograr el fin propuesto

5.3.4. Método Comparativo

Este método me permitió diferenciar realidades jurídicas en Derecho comparado, realice un estudio a diferentes legislaciones, accediendo a diferenciar realidades legales de legislaciones internacionales que tipifica y sanciona la estafa informática como delito autónomo, como la ley penal alemana, el Código Penal Español y el Convenio de Ciberdelincuencia celebrado en Budapest para países europeos.

6. Resultados de la Investigación de Campo

6.1. Resultados de las Encuestas

Para la obtención de los resultados de la presente investigación se aplicó treinta encuestas a profesionales del Derecho de la ciudad de Loja, de forma directa quienes manifestaron su opinión acerca del tema investigado, las que me sirvieron para realizar la contratación de la hipótesis; así como la verificación de los objetivos planteados, obteniendo de esta forma resultados significativos, que los detallo a continuación.

Pregunta 1

¿Conoce usted el delito de estafa común?

Indicadores	Variables	Porcentaje
Si	30	100%
No	0	0%

Tabla 1 Conocimiento de la estafa común

Fuente: Encuestas realizadas a profesionales del derecho

Autora: Claudia Karina Medina González

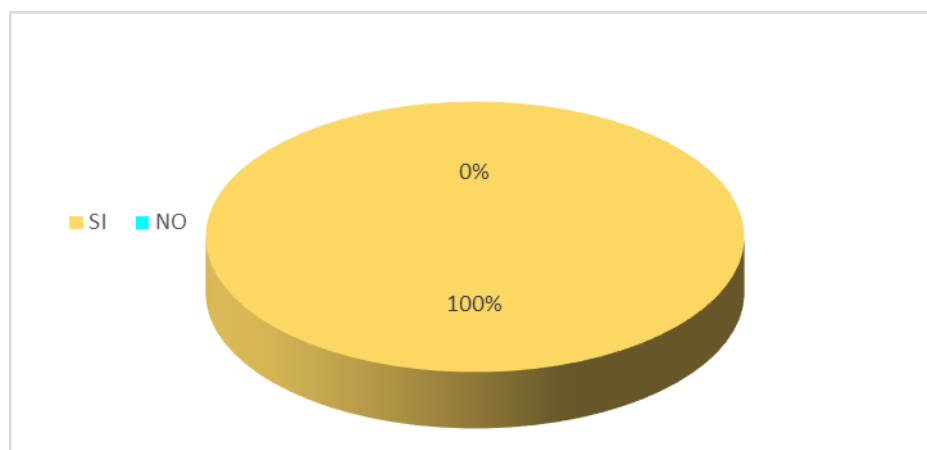


Ilustración 3 Conocimiento del delito de estafa común

Fuente: Encuestas realizadas a profesionales del derecho

Autora: Claudia Karina Medina González

Interpretación:

Como se desprende los datos del cuadro Nro. 1, ilustración Nro. 3 de la población muestra de treinta profesionales del Derecho encuestados, en su totalidad manifestaron que, si conocen e identifican el delito de estafa común, lo que representan un porcentaje de 100% de la población muestra.

Análisis:

Por las respuestas obtenidas en la primera interrogante de la encuesta es fácil deducir que todo profesional de Derecho, tiene claro lo que es el delito de estafa común, y en adición se puede deducir que conoce perfectamente su ubicación en nuestra legislación penal, concretamente en el Art. 186, el mismo que abarca elementos básicos como son el error, el engaño y el daño al bien patrimonial.

Pregunta 2

¿Tiene conocimiento usted si en el Ecuador está tipificado el delito de estafa informática?

Indicadores	Variables	Porcentaje
Si	0	0%
No	30	100%

Tabla 2 No tipificación del delito de estafa informática

Fuente: Encuestas realizadas a profesionales del derecho

Autora: Claudia Karina Medina González

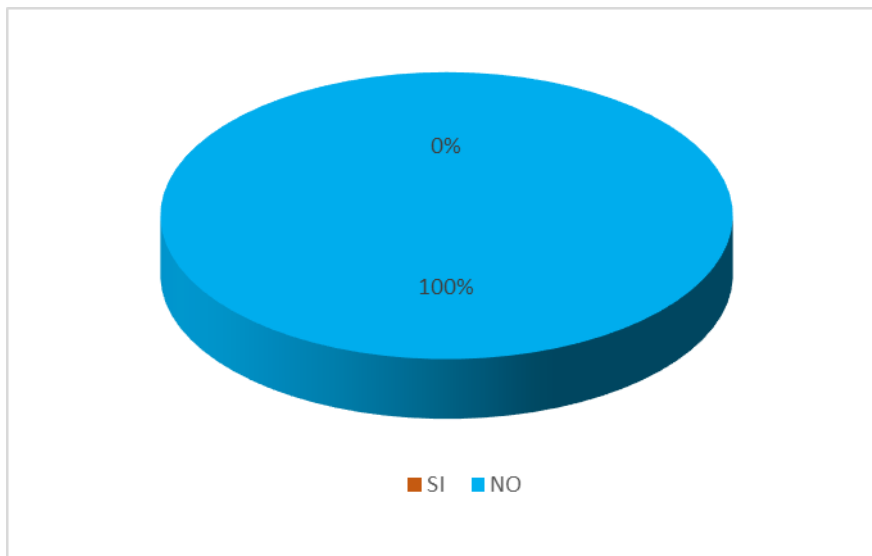


Ilustración 4 No tipificación del delito de estafa informática en la Legislación Ecuatoriana

Fuente: Encuestas realizadas a profesionales del derecho

Autora: Claudia Karina Medina González

Interpretación:

En la tabla Nro. 2, ilustración Nro. 04, con los datos evidenciados de los 30 profesionales del Derecho encuestados, en su totalidad respondieron que no tenían conocimiento de que el delito de estafa informática se encontrará como tal en el catálogo de delitos del COIP lo que hace referencia a que no está tipificado en el Código Orgánico Integral Penal, conformando un 100% en la uniformidad de las respuestas manifestadas en la interrogante realizada.

Análisis:

Los profesionales del Derecho encuestados en este trabajo de investigación, tienen conocimiento de que el delito de estafa informática representa una ausencia en nuestro Código Orgánico Integral Penal. Que el delito como tal de manera autónoma no figura en nuestra legislación penal por tanto afirmamos nuestro planteamiento que

esta falta de tipificación deja espacio para la vulneración de bienes jurídico protegidos.

Pregunta 3

¿Considera usted que existen diferencias entre el delito de estafa común y estafa informática? ¿Cuáles?

Indicadores	Variables	Porcentaje
Si	27	90%
No	3	10%

Tabla 3 Existencia de diferencias entre estafa común y delito informático

Fuente: Encuestas realizadas a profesionales del derecho

Autora: Claudia Karina Medina González

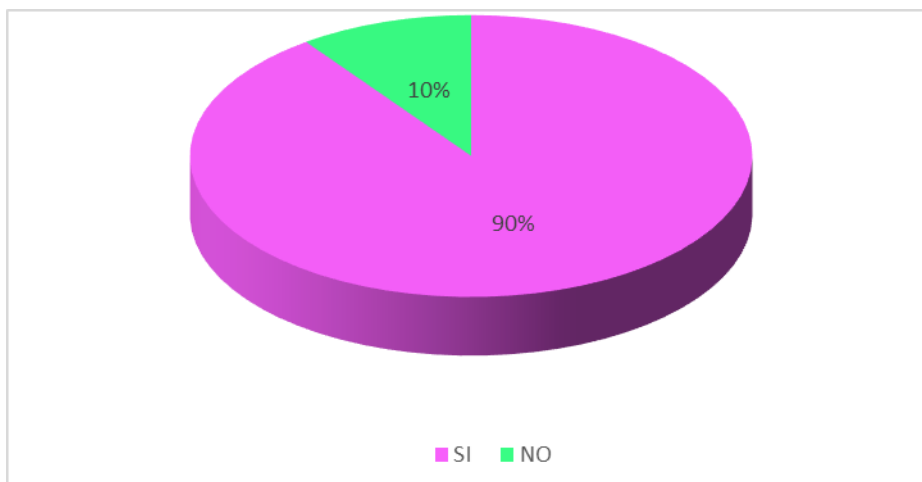


Ilustración 5 Existencia de diferencias entre estafa común y delito informático

Fuente: Encuestas realizadas a profesionales del Derecho

Autora: Claudia Karina Medina González

Interpretación:

Como se puede evidenciar en la tabla Nro. 03, ilustración Nro. 05, con la tabulación de las respuesta de la población muestra del trabajo de campo, que son los 30 profesionales del Derecho encuestados, 27 de ellos respondieron que si existía diferencias entre el delito de estafa común y estafa informática, manifestando que la principal diferencia está en la forma de realizar el ilícito es decir en el modo de

operar o proceder de la acción delictiva y 3 de ellos señalaron que no existe ninguna diferencia, debido a que consideran que solo cambia el medio de operar mas no el fin; en los otros casos los encuestados no supieron dar su opinión al respecto de la pregunta realizada. Lo que en porcentajes representaría que el 90% de los encuestados concuerdan que existe diferencias entre ambos delitos y un 10% opinan de manera negativa.

Análisis

En base a las respuestas de esta pregunta se puede evidenciar que la mayoría de los profesionales del Derecho efectivamente tienen conocimiento de que existen ciertas diferencias entre ambos delitos. La más importante que es pertinente mencionar en el caso de la estafa informática que para su cometimiento se utilizan medios informáticos. En cambio en la estafa común las víctimas si identifican a su estafador, porque existe un contacto directo entre el estafador y la víctima, mientras que en la estafa informática, la víctima no logra identificar a su estafador, ya se lo puede ejecutar a través de medios informáticos, como el internet, redes sociales, servicios móviles, etc., es decir, el estafador se encuentra detrás de un medio informático, además la población muestra encuestada concuerdan con la idea, que la estafa común únicamente tipifica el daño patrimonial provocado a través de cajeros bancarios pero que no abarca las modalidades de otros tipos de estafa informática, de esta manera queda claro que la estafa informática no puede ser sancionada dentro del tipo de estafa común. Por otra parte, dentro de las respuestas a esta interrogante, quienes manifestaron que no existían diferencias entre ambos delitos lo señalan así en razón que al utilizar diferentes medios para el cometimiento de la infracción pero que el daño producido es el mismo. Ciertamente si existe una diferencia y como tal no se

puede sancionar o subsumir la conducta a otro tipo penal dado que en virtud de la misma legislación penal ecuatoriana en su Art. 13, numeral 2, establece que los tipos penales se interpretarán en forma estricta, esto es, respetando el sentido literal de la norma.

Pregunta 4

¿Cree que es necesario tipificar en el Código Orgánico Integral Penal como delito autónomo a la estafa informática y sus modalidades?-*La inserción de enlaces fraudulentos en redes sociales y correos electrónicos por parte del estafador, para obtener información personal y confidencial denominada **Phishing**, - La inserción de enlaces o mensajes fraudulentos a través de la telefonía móvil, para obtener información personal y confidencial, sea a través de mensajes de texto o WhatsApp denominado **Smishing**; y, -Las llamadas programadas de forma simultáneas a diferentes números mediante el cual obliga al usuario a llamar al número asignado so pena de ver perjudicado su patrimonio en su cuenta bancaria denominada **Vishing**, toda la información obtenida por el estafador es insertada por la víctima de forma voluntaria.*

Indicadores	Variables	Porcentaje
Si	26	87%
No	4	13%

Tabla 4 Apoyo a la tipificación del delito de estafa informática y sus modalidades

Fuente: Encuestas realizadas a profesionales del derecho

Autora: Claudia Karina Medina González

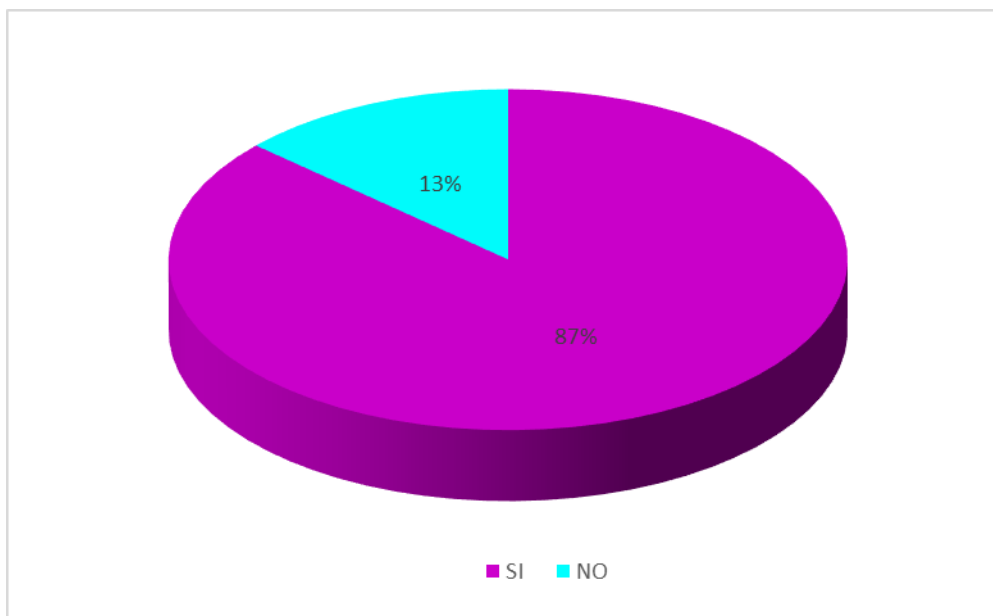


Ilustración 6 Apoyo a la tipificación del delito de estafa informática y sus modalidades

Fuente: Encuestas realizadas a profesionales del Derecho

Autora: Claudia Karina Medina González

Interpretación:

Como se desprenden de los datos reflejados en la tabla Nro. 04, ilustración Nro. 06, de los 30 profesionales del Derecho encuestados, con respecto a la cuarta pregunta planteada 26 de ellos manifestaron que, se encuentran totalmente de acuerdo que la figura de estafa informática y sus modalidades sea tipificada como delito autónomo en el Código Orgánico Integral Penal, y 4 de ellos respondieron que no están de acuerdo, argumentado su respuesta negativa en base que se lo puede agregar al delito de estafa común tipificado en el Art. 186, o que se puede subsumir a otro tipo penal. Lo que en porcentajes representa que un 87% de los encuestados concuerdan que debe tipificarse autónomamente y un 13% cree que se debe adecuar a otro tipo penal o a su vez agregarse al Art. 186.

Análisis.

Con los resultados y opiniones emitidas por los profesionales del Derecho encuestados, efectivamente se evidencia la necesidad de establecer un tipo penal con el que se pueda sancionar a la acción ejecutada de manera autónoma, sin necesidad de estar adecuando a otros tipos penales similares, ya que a medida que las tecnologías avanzan y evolucionan las nuevas formas de delinquir también lo hacen, y, en ese contexto el Derecho también debe evolucionar e ir a la par de la evolución de la Sociedad de acuerdo a la necesidad y realidad social. Además, la tipificación como delito autónomo procura para dar cumplimiento al principio de legalidad, para que la persona que cometió el ilícito sea sancionada y no sea una acción delictiva quede en la impunidad.

Es de considerar que estas conductas no se pueden subsumir en otro tipo penal ya que recordemos que la misma ley establece que ésta será interpretada en forma estricta, esto es, respetando el sentido literal de la norma. Y aún más importante los elementos del delito de estafa común no se subsumen a los de la estafa informática y esto actualmente permite la existencia de vacíos legales que afectan a las personas y su patrimonio por una correcta tipificación para una mejor administración de justicia.

Pregunta 5

¿Considera usted que al tipificar las modalidades de estafa informática en el Código Orgánico Integral Penal ecuatoriano se protegería el patrimonio de los ciudadanos?

Indicadores	Variabes	Porcentaje
Si	27	90%
No	3	10%

Tabla 5 Protección del patrimonio con la tipificación del delito de estafa informática

Fuente: Encuestas realizadas a profesionales del Derecho

Autora: Claudia Karina Medina González

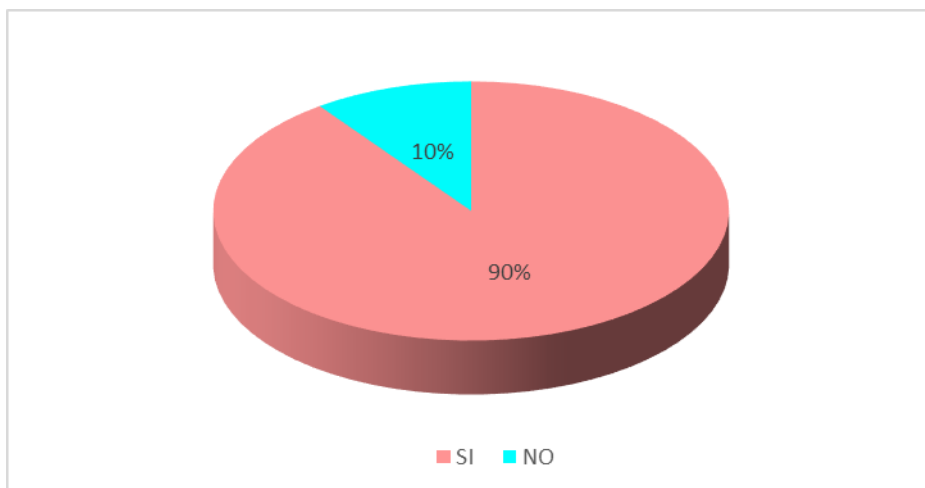


Ilustración 7 Protección del patrimonio con la tipificación del delito de estafa informática

Fuente: Encuestas realizadas a profesionales del Derecho

Autora: Claudia Karina Medina González

Interpretación:

Como se puede demostrar en los datos de la tabla Nro. 05, ilustración No. 07, de los 30 profesionales del Derecho encuestados, de la muestra de población base 27 de ellos respondieron de manera afirmativa a esta interrogante debido a que, de llegarse a estar tipificado el delito de estafa informática, se protege el patrimonio de las personas que es la principal afectación en este tipo de delitos, mientras tanto 3 de ellos, respondieron de manera negativa debido a que consideran que no se protegería de otra forma que la actual teniendo en cuenta que se puede adecuar a otro tipo penal a la acción y que el cuidado de los bienes proviene de la necesidad y el deber de precaución de proteger cada quien lo suyo. Además, consideran que al realizar esta modificación en la ley penal se podría producir una modificación del delito de estafa común. En conclusión, referente a los datos arrojados representa en proporciones que un 90% de los encuestados concuerdan que si protege el patrimonio y un 10% que no.

Análisis:

Al ser la estafa informática un delito contra el patrimonio y al encontrarse tipificado como delito en nuestra legislación penal, concuerdo con las respuestas mayoritarias emitidas por los encuestados, en razón de que considero que efectivamente si se protegería a un bien jurídico protegido y que de la misma forma se previene que dicha acción sea cometa por el temor a recibir una coerción. Al mismo tiempo es de considerar que las posibles víctimas podrán tener conocimiento acerca de esta modalidad de estafa y tener mayor cuidado al momento de ingresar a páginas de dudosa procedencia y entregar información personal en las mismas, pero teniendo la certeza de que son amparados por una legislación penal y en el caso de ser víctimas la administración de justicia procederá.

Creando de esta manera la posibilidad de que las personas, víctimas de este delito puedan exigir y recurrir al sistema penal para que su Derecho vulnerado sea restituido y el sujeto activo reciba la oportuna y adecuada sanción. A mi criterio no comparto la postura de algunos profesionales del Derecho expresada en la interrogante planteada acerca de que se debe adecuar esta acción a la que nos referimos en otro tipo penal, es de recordar y hacer mención nuevamente que el Derecho Penal establece que de la norma será interpretada literalmente a lo estipulado en ella, tampoco se podría modificar el delito de estafa común e incluirla a este tipo penal ya que cada tipo maneja un verbo rector específico y autónomo.

6.2. Resultados de las Entrevistas

Con la finalidad de verificar la realidad socio-jurídica de la problemática planteada dentro de la presente investigación y obtener criterios que me permitan comprobar

los objetivos planteados, aplicando así los lineamientos metodológicos de la investigación de campo se elaboró preguntas de carácter abierto y otras más específicas, relacionadas al tema, problema, objetivos e hipótesis; estas interrogantes fueron dirigidas tres profesionales del Derecho de libre ejercicio especialistas en Derecho penal. Obteniendo los siguientes resultados.

Entrevista #1

Entrevistado: Magister Abogado Juan Méndez.

Pregunta 1

Con los elementos fundamentales que configuran el delito de Estafa Común tipificado en el art. 186 del Código Orgánico Integral Penal y los elementos que en doctrina señala como indispensables para que exista estafa informática encontrándose este último no tipificado en el Código Orgánico Integral Penal ¿Considera Ud. que hay diferencias entre estos dos tipos de estafa?

Estafa Común:

El delito de Estafa Común tipificada en el Artículo 186 del Código Orgánico Integral Penal producido por parte del estafador hacia la víctima presenta aspectos fundamentales como es el engaño, el daño al bien patrimonial y *específicamente en numeral 2 del mismo se limita solo a la alteración, clonación, adulteración o modificación de dispositivos originales de cajeros bancarios.*

Estafa Informática

Presenta los siguientes aspectos: a.- Manipulación fraudulenta de los elementos informáticos, b.- Presencia de sistemas informáticos, c.- Obtención de beneficio ilícito; y, d.- Perjuicio económico no cuantificable.

El abogado manifiesta en palabras textuales que: a mi opinión profesional, sí, considero que existen claras diferencias entre ambos tipos de estafa que plantea.

¿Por qué? Argumente su respuesta:

Doctrinariamente para que se genere o produzca el delito de estafa, tiene que haber cierto engaño, inducir al error a una persona y para causarle un perjuicio personal; ya sea esto se efectuó de manera directa o indirecta, si no hay estos tres elementos consecutivos propios del delito de estafa no estaríamos refiriéndonos a la estafa. Sea que se trate de la estafa común o de la estafa informática deben tener estos tres elementos comunes que menciono; pero la diferencia entre estos dos tipos de delitos recae en: la estafa común no se utiliza medios informáticos para su cometimiento a diferencia de la estafa informática que, si se usa de ellos, principalmente el recurso más usado es lo que conocemos por internet, que llevado a la realidad jurídica genera cierto problema al momento de sancionar. Es muy importante tener en cuenta el principio de legalidad lo que nos conduce a que debería estar tipificada la estafa cuando se utilice medios informáticos, con la utilización de equipos informáticos o cualquier otro medio electrónico empleado con el objeto de efectuar engaño o inducir al error y como lo he mencionado ocasionar el perjuicio al patrimonio económico de las personas víctimas de estas modalidades delictivas.

Tomando en cuenta que para cualquier modalidad de estafa es necesario que exista el engaño, considera usted que ¿Se podría argumentar que es debido a un error en virtud de, que la computadora o el medio electrónico indujo a el error?

Pues si bien es cierto para que se produzca el engaño u error previamente debe existir una manipulación informática ya que a través de estos medios es que se produce o se lleva a el engaño a la persona convirtiéndola en la víctima, es de mencionar que la responsabilidad penal no recae sobre un equipo o sistema informático si no en la persona que lo manipulo dado que sin la manipulación humana no se producirían estos efectos.

Pregunta 2

En la doctrina, en fuentes informáticas y en algunas legislaciones extranjeras la estafa informática presenta las siguientes modalidades:

Phishing. - Es la inserción de un link fraudulento en redes sociales y e-mail por parte del estafador, para obtener información personal y confidencial, insertada por la víctima de forma voluntaria.

Smishing. - Es la inserción de enlaces o mensajes fraudulentos a través de la telefonía móvil, para obtener información personal y confidencial, ingresada por la víctima ya sea a través de mensajes de texto o aplicaciones de intercambio de textos como WhatsApp.

Vishing. - Son llamadas programadas de forma simultáneas a diferentes números mediante el cual obliga al usuario a llamar al número asignado so pena de ver perjudicado su patrimonio en su cuenta bancaria.

Como elemento importante es de resaltar que estas modalidades de DELITO NO SE ENCUENTRAN TIPIFICADOS EN EL CÓDIGO ORGÁNICO INTEGRAL PENAL, la Estafa Común tipificada en el Código Orgánico Integral Penal en el Artículo 186 es general que solo consta de dos elementos engaño, daño patrimonial, y *específicamente en numeral 2 del mismo se limita solo a la alteración, clonación, adulteración o modificación de dispositivos originales de cajeros bancarios*. Con estos elementos anotados apelo a su criterio especializado para que digno en argumentar, si usted ¿considera necesario el que se implemente en el Código Orgánico Integral Penal el delito de Estafa Informática y sus modalidades que son consecuencia de los avances científicos y tecnológicos?

Si, considero que es importante que se dé la tipificación de la estafa informática y todas sus modalidades hasta ahora conocidas, basándonos en el principio de legalidad que he hecho alusión; pues si no está tipificado como tal, no puede ser una persona responsable penalmente por el cometimiento de dichas acciones, lo que en latín llamamos “**nulla lege sine lege**”, es decir, si no está enmarcado en la ley no se puede sancionar a una persona.

Y esto de singularizar cada una de las modalidades de la estafa informática es muy importante para poder determinar la infracción penal; en qué forma se la ejecuto y obviamente conjuntamente a ella se deberá estipular la sanción correspondiente y equivalente al daño que se causa.

Usted dentro de su carrera y experiencia profesional como abogado de libre ejercicio ¿ha tenido casos de este tipo de estafa?

Si, efectivamente he tenido este tipo de actos ilícitos; pero lastimosamente no se lo ha podido judicializar de la manera correcta o como lo que constituyen como tal estafa informática. Cuando Fiscalía General del Estado formula cargos en su mayoría, lo hace como un delito de perjuicio o engaño al consumidor, en otras ocasiones como el delito de estafa común, tipificados en el Artículo 235 y 186 respectivamente del COIP, o a su vez los consideran dentro de delitos contra el régimen monetario enmarcados en los Artículos 304, 305, y 306 específicamente de la ley mencionada; el mismo que no corresponde a la forma de cometer el ilícito sino a un delito de estafa informática ya que cumple todos los elementos consecutivos porque existe el engaño, el error, el daño al bien patrimonial y la utilización de medios informáticos, es decir, se comete el ilícito a través de este. Considero que estos errores se dan porque no está de una manera taxativa determinada en el Código Orgánico Integral Penal la estafa informática, por ello, el Fiscal se ve en la necesidad de acoplar la conducta a una figura que se asemeje a la realidad procesal.

Pregunta 3

Con los elementos antes mencionados ¿considera usted que para que se genere el delito de Estafa Informática es indispensable la manipulación de los dispositivos tecnológicos (hardware y software)?

Si, considero que es la base para que se pueda realizar la estafa informática, si no tenemos las herramientas necesarias en estos casos el hardware, el software y la programación respectiva, la conducta no correspondería a estafa informática; ya que en Derecho Penal se juzga la conducta.

Pregunta 4

¿Considera usted que, con el avance de las Tecnologías de la Información y la Comunicación, el delito de estafa común tipificado en el Código Orgánico Integral Penal no abarca lo que en su totalidad constituye la Estafa Informática?

Realmente la estafa común no abarca lo que constituye la estafa informática, convirtiéndose este vacío en una tarea para el legislador, según la Constitución de la República de Ecuador en su Artículo 132, numeral 2, referente a la reserva de ley y que el asambleísta tiene como tarea tipificar estos hechos, entonces, es necesario determinar y tipificar la estafa informática de manera taxativa en el Código Orgánico Integral Penal para que se pueda de una u otra forma no dejar en la impunidad los delitos informáticos muy comunes hoy en día.

Pregunta 5

¿Según su criterio profesional, se debería tipificar en el Código Orgánico Integral Penal el delito de Estafa Informática como delito autónomo, por tener elementos propios que no se subsumen en el delito de Estafa Común?

Si, siempre y cuando sea ubicado dentro del mismo catálogo de los delitos de estafa que abarca el daño al patrimonio. Es importante además tomar en consideración que en la legislación penal ecuatoriana dentro del Artículo 13, numeral 2, se establece que la norma sea interpretada de manera literal, y en su numeral 3 se señal que únicamente se permitirá analogías en favor del procesado y no en su contra.

Entrevista #2

Entrevistado: Magister Abogado Bayron Camacho.

Pregunta 1

Con los elementos fundamentales que configuran el delito de Estafa Común tipificado en el art. 186 del Código Orgánico Integral Penal y los elementos que en doctrina señala como indispensables para que exista estafa informática encontrándose este último no tipificado en el Código Orgánico Integral Penal ¿Considera Ud. que hay diferencias entre estos dos tipos de estafa?

Estafa Común:

El delito de Estafa Común tipificada en el Artículo 186 del Código Orgánico Integral Penal producido por parte del estafador hacia la víctima presenta aspectos fundamentales como es el engaño, el daño al bien patrimonial y *específicamente en numeral 2 del mismo se limita solo a la alteración, clonación, adulteración o modificación de dispositivos originales de cajeros bancarios.*

Estafa Informática

Presenta los siguientes aspectos: a.- Manipulación fraudulenta de los elementos informáticos, b.- Presencia de sistemas informáticos, c.- Obtención de beneficio ilícito; y, d.- Perjuicio económico no cuantificable.

El profesional entrevistado manifiesta: desde el punto de vista planteado con los argumentos expuestos en la pregunta; si considero que existen algunas diferencias entre ambos tipos de estafa que manifiesta.

¿Por qué? Argumente su respuesta:

Porque hay que tener presente que en la estafa común no se utilizan medios o equipos informáticos y en la estafa informática si son los esenciales para su cometimiento, principalmente a través del internet.

Tomando en cuenta que para cualquier modalidad de estafa es necesario que exista el engaño, considera usted que ¿Se podría argumentar que es debido a un error en virtud de, que la computadora o el medio electrónico indujo a el error?

Considero que no, para que un aparato o artefacto electrónico opere realizando tareas puntuales es necesario del componente humano y que emita la programación correspondiente u ordene la acción. Aquí se refleja que no hay un espacio para considerar el error puesto que hay voluntad, finalidad y la fuerza física humana puesta en movimiento que plantea el camino y los medios de obtención del resultado propuesto, estos elementos en la teoría del delito son los definen a la acción.

Pregunta 2

En la doctrina, en fuentes informáticas y en algunas legislaciones extranjeras la estafa informática presenta las siguientes modalidades:

Phishing. - Es la inserción de un link fraudulento en redes sociales y e-mail por parte del estafador, para obtener información personal y confidencial, insertada por la víctima de forma voluntaria.

Smishing. - Es la inserción de enlaces o mensajes fraudulentos a través de la telefonía móvil, para obtener información personal y confidencial, ingresada por la víctima ya sea a través de mensajes de texto o aplicaciones de intercambio de textos como WhatsApp.

Vishing. - Son llamadas programadas de forma simultáneas a diferentes números mediante el cual obliga al usuario a llamar al número asignado so pena de ver perjudicado su patrimonio en su cuenta bancaria.

Como elemento importante es de resaltar que estas modalidades de DELITO NO SE ENCUENTRAN TIPIFICADOS EN EL CÓDIGO ORGÁNICO INTEGRAL PENAL, la Estafa Común tipificada en el Código Orgánico Integral Penal en el Artículo 186 es general que solo consta de dos elementos engaño, daño patrimonial, y *específicamente en numeral 2 del mismo se limita solo a la alteración, clonación, adulteración o modificación de dispositivos originales de cajeros bancarios.* Con estos elementos anotados apelo a su criterio especializado para que digno en argumentar, si usted ¿considera necesario el que se implemente en el Código Orgánico Integral Penal el delito de Estafa Informática y sus modalidades que son consecuencia de los avances científicos y tecnológicos?

Sí, yo considero que es importante que se tipifique de la estafa informática en nuestro Código Penal, tomando en consideración los avances tecnológicos con su debido respaldo en términos técnicos para la mayoría muchos de ellos desconocidos; para que pueda ser juzgado las acciones que se constituyen en delictivas, su tipificación puede ejecutarse en el amparo del principio de legalidad dado pues, que si no está tipificado como delito en la norma no puede ser una persona responsable penalmente; el hecho de que se encuentre singularizado cada modalidad es muy importante para poder determinar la infracción penal y en qué forma se la ejecuta.

Usted dentro de su carrera y experiencia profesional como abogado de libre ejercicio ¿ha tenido casos de este tipo de estafa?

Debo indicar que en mi consultorio jurídico no han sido casos comunes, la mayoría de personas víctimas de estos actos generalmente no suelen denunciar, cuando se trata de afectación de cuentas bancarias tratan con el banco emisor de su tarjeta de crédito o donde tienen su cuenta bancaria, no resolviendo nada y donde terminan asumiendo el sobregiro de su tarjeta de crédito estas personas principalmente no acuden a la administración de justicia por el desconocimiento de que este tipo de actos pueden y deben ser sancionados. En los casos de las personas que acuden por asesoría legal y plantean la denuncia los casos como tal no son sentenciados como estafa informática sino como estafa común y según ciertos aspectos de los hechos se busca acoplar a otros tipos de delitos.

Pregunta 3

Con los elementos antes mencionados ¿considera usted que para que se genere el delito de Estafa Informática es indispensable la manipulación de los dispositivos tecnológicos (hardware y software)?

Lógicamente que es indispensable la manipulación de dispositivos tecnológicos ya que los dispositivos tecnológicos se constituyen en un medio por cual el infractor se vale de ellos para cometer el delito.

Pregunta 4

¿Considera usted que, con el avance de las Tecnologías de la Información y la Comunicación, el delito de estafa común tipificado en el Código Orgánico

Integral Penal no abarca lo que en su totalidad constituye la Estafa Informática?

La evolución del Derecho necesariamente debe ir acorde a la evolución de la Sociedad, basado en eso considero que necesario que se tipifique el delito de estafa informática con un verbo rector propio. Recordemos que el Derecho es cambiante este evoluciona de acuerdo a la misma Sociedad por cuanto su cambio es necesario.

Pregunta 5

¿Según su criterio profesional, se debería tipificar en el Código Orgánico Integral Penal el delito de Estafa Informática como delito autónomo, por tener elementos propios que no se subsumen en el delito de Estafa Común?

Si considera que se debería tipificar autónomamente, ya que si se lo incluye junto al delito de estafa común no tendría sentido su tipificación si se va usar el mismo verbo rector.

Entrevista #3

Entrevistado: Magister Abogada Alexandra Encarnación Díaz.

Pregunta 1

Con los elementos fundamentales que configuran el delito de Estafa Común tipificado en el art. 186 del Código Orgánico Integral Penal y los elementos que en doctrina señala como indispensables para que exista estafa informática encontrándose este último no tipificado en el Código Orgánico Integral Penal

¿Considera Ud. que hay diferencias entre estos dos tipos de estafa?

Estafa Común:

El delito de Estafa Común tipificada en el Artículo 186 del Código Orgánico Integral Penal producido por parte del estafador hacia la víctima presenta aspectos fundamentales como es el engaño, el daño al bien patrimonial y *específicamente en numeral 2 del mismo se limita solo a la alteración, clonación, adulteración o modificación de dispositivos originales de cajeros bancarios.*

Estafa Informática

Presenta los siguientes aspectos: a.- Manipulación fraudulenta de los elementos informáticos, b.- Presencia de sistemas informáticos, c.- Obtención de beneficio ilícito; y, d.- Perjuicio económico no cuantificable.

La abogada responde que: si, considero que, si bien ambos tipos de estafa están enfocados a dirigir un daño patrimonial, es claramente que entre los dos hay diferencias existentes.

¿Por qué? Argumente su respuesta:

Porque en el delito de estafa común no hay la presencia de elementos informáticos si bien en la legislación contempla la clonación de tarjetas hoy en día los delitos de estafa informática van más allá, como el suplantar a un funcionario de la identidad bancaria enviando formularios para obtener información o conseguir transferencias bancarias a través de estas modalidades.

Tomando en cuenta que para cualquier modalidad de estafa es necesario que exista el engaño, considera usted que ¿Se podría argumentar que es debido a un error en virtud de, que la computadora o el medio electrónico indujo a el error?

No, con los conocimientos básicos que poseo en informática tengo toda la seguridad para decir que un programa o un artefacto informático, jamás va a operar sin una orden previa; es así que la estafa es planeada y ejecutada por una persona con el uso de esas herramientas informáticas.

Pregunta 2

En la doctrina, en fuentes informáticas y en algunas legislaciones extranjeras la estafa informática presenta las siguientes modalidades:

Phishing. - Es la inserción de un link fraudulento en redes sociales y e-mail por parte del estafador, para obtener información personal y confidencial, insertada por la víctima de forma voluntaria.

Smishing. - Es la inserción de enlaces o mensajes fraudulentos a través de la telefonía móvil, para obtener información personal y confidencial, ingresada por la víctima ya sea a través de mensajes de texto o aplicaciones de intercambio de textos como WhatsApp.

Vishing. - Son llamadas programadas de forma simultáneas a diferentes números mediante el cual obliga al usuario a llamar al número asignado so pena de ver perjudicado su patrimonio en su cuenta bancaria.

Como elemento importante es de resaltar que estas modalidades de DELITO NO SE ENCUENTRAN TIPIFICADOS EN EL CÓDIGO ORGÁNICO INTEGRAL PENAL, la Estafa Común tipificada en el Código Orgánico Integral Penal en el Artículo 186 es general que solo consta de dos elementos engaño, daño patrimonial, y específicamente en numeral 2 del mismo se limita solo a la alteración, clonación, adulteración o modificación de dispositivos

originales de cajeros bancarios. Con estos elementos anotados apelo a su criterio especializado para que digne en argumentar, si usted ¿considera necesario el que se implemente en el Código Orgánico Integral Penal el delito de Estafa Informática y sus modalidades que son consecuencia de los avances científicos y tecnológicos?

Definitivamente es necesario, a lo largo de la Carrera de Derecho nuestros docentes constantemente nos repiten el Derecho es cambiante, palabras que en la práctica profesional se vuelven reales. Nos encontramos maravillados con todo lo que la tecnología e informática puede hacer por nosotros, pero hemos dejado descuidado de los peligros que también vienen con ellos. Es por eso que el Derecho debe evolucionar de acuerdo a la Sociedad y hoy en día vivimos en una Sociedad donde prima lo informático.

Usted dentro de su carrera y experiencia profesional como abogado de libre ejercicio ¿ha tenido casos de este tipo de estafa?

Sí, me encontrado con ciertos casos similares, que generalmente son resueltos por el sistema de justicia como delito de estafa común.

Pregunta 3

Con los elementos antes mencionados ¿considera usted que para que se genere el delito de Estafa Informática es indispensable la manipulación de los dispositivos tecnológicos (hardware y software)?

Sí la manipulación de estos dispositivos es indispensable es lo que le da la característica de informático de no ser el medio para el cometimiento de este tipo de delitos, estaríamos frente a un delito de estafa común.

Pregunta 4

¿Considera usted que, con el avance de las Tecnologías de la Información y la Comunicación, el delito de estafa común tipificado en el Código Orgánico Integral Penal no abarca lo que en su totalidad constituye la Estafa Informática?

El delito de estafa común en el catálogo de delitos del COIP con los verbos rectores establecidos no están adecuados para enmarcar a todo lo que corresponde el delito de estafa informática y sus modalidades, estos deberían ser tipificados de una forma muy aparte.

Pregunta 5

¿Según su criterio profesional, se debería tipificar en el Código Orgánico Integral Penal el delito de Estafa Informática como delito autónomo, por tener elementos propios que no se subsumen en el delito de Estafa Común?

Si considero que es necesaria la modificación al Código Orgánico Integral Penal, debido a que el actual catálogo de delitos no responde a la realidad social y a sus avances tecnológicos, por lo tanto, no se está protegiendo derechos, ni el patrimonio de las personas y mucho menos se está sancionando como correspondería por estos delitos en razón de que los administradores de justicia lo interpretan como delitos de estafa común.

Análisis de las entrevistas:

De las entrevistas realizadas a los profesionales del derecho se puede determinar que creen en la existencia diferencias muy marcadas entre el delito de estafa común y la estafa informática por las siguientes razones: en la estafa común no se utilizan

medios o equipos informáticos y en la estafa informática si son los esenciales para su cometimiento, principalmente a través del internet, y que un aspecto tener siempre presente es el hecho de que para un aparato o artefacto electrónico opere realizando tareas puntuales es necesario del componente humano y que emita la programación correspondiente u ordene la acción en este caso delictiva.

De sus opiniones en manera conjunta se logró determinar que es importante que se tipifique de la estafa informática y todas sus modalidades en nuestro Código Penal, tomando en consideración los avances tecnológicos con su debido respaldo en términos técnicos para la mayoría muchos de ellos desconocidos; en base al principio de legalidad considerando que si no está tipificado como delito en la norma no puede ser una persona responsable penalmente; es decir, si no está enmarcado en la ley no se puede sancionar a una persona. Además de ello su tipificación tendría un carácter de urgente considerando que los avances tecnológicos se dan a una gran velocidad y así al amparo de la ley poder determinar la infracción penal y en qué forma se la sanciona.

7. Discusión

7.1. Verificación de Objetivos

Con la finalidad de verificar el cumplimiento de los objetivos planteados en la presente investigación, sobre la temática abordada “LA FALTA DE TIPIFICACIÓN DEL DELITO DE ESTAFA INFORMÁTICA EN EL CÓDIGO ORGÁNICO INTEGRAL PENAL (COIP), PERJUDICA EL PATRIMONIO DE LAS PERSONAS”, por objetivo general establecí uno de fundamental valor y tres objetivos secundarios con la misma importancia. Es por ello que afianzada en él un

estudio teórico-normativo realizado y en conjunto con los datos arrojados por la investigación de campo realizada; satisfactoriamente he obtenido los resultados que exponen la necesidad de tipificar el delito de estafa informática como un delito autónomo al delito de estafa común; es así que para una correcta verificación de lo comprobado realizo los siguientes análisis y contrastes:

7.1.1. Objetivo General.

“Realizar un estudio teórico, doctrinario y jurídico del delito de estafa para demostrar que la tipificación general del Artículo 186 numeral 2 del Código Orgánico Integral Penal (COIP) no abarcan las conductas de estafa informática, y es necesario tipificarlas en la legislación penal ecuatoriana”.

Mediante la revisión de la literatura este objetivo pudo ser verificado, se realizó un compendio selectivo de fuentes de información para los marcos conceptual, doctrinario, jurídico y una comparación de legislaciones penales de otros países, así como convenios y tratados internacionales; con los cuales he permitido demostrar los delitos informáticos no son contemplados en la legislación penal ecuatoriana vigente, concluyendo que esta ausencia de tipificación permite que se presenten situaciones o acciones delictivas a través de medios o aparatos informáticos que producen daños al patrimonio de las personas.

Con la investigación de campo, en base a las respuestas presentadas por los profesionales del Derecho en las encuestas y entrevistas, existe el conocimiento de las afectaciones que ocasionan los delitos informáticos y que no existen dentro del catálogo de delitos del COIP como tal y de manera autónoma.

7.1.2. Objetivos Específicos.

“Realizar un estudio teórico, normativo y doctrinario del delito de estafa para contrastar con el Derecho comparado la nueva tipificación de la estafa informática en el desarrollo de las Tecnologías de la Información y la Comunicación que no se encuentra tipificado en el Código Orgánico Integral Penal (COIP)”.

Este objetivo se verificó su cumplimiento de una manera positiva, por medio del análisis del Derecho Comparado extrayendo el articulado más esencial referente al tema y con las opiniones de expertos acerca de la evolución de las tecnologías de información y como son un medio para la ejecución de actividades delictivas. Con este apoyo reunido se verificó que este delito no se encuentra como estafa informática en el Código Orgánico Integral Penal y que, por ende, su tipificación resultaría muy conveniente a la realidad jurídica de nuestro país, en razón de que le apoyan ciertos principios importantes establecidos como el de legalidad.

“Determinar que existe confusión entre el delito de estafa común y estafa informática”.

Para la verificación de este objetivo específico, me basé en los datos obtenidos a través de la aplicación de las encuestas y entrevistas donde pude determinar que en la práctica procesal, la estafa informática es confundida y adecuada al delito de estafa común o en su defecto a otros delitos semejantes; en razón de no encontrarse como tal en la legislación penal.

“Elaborar propuesta de reforma al Código Orgánico Integral Penal (COIP), en el que se incorpore el delito de Estafa Informática”.

Este objetivo se cumple a su cabalidad porque la mayoría de la población muestra de la investigación de campo realizada, coinciden en sus respuestas en las preguntas referentes a la necesidad de reformar el Código Orgánico Integral Penal para incluir en el catálogo de delitos a la estafa informática; manifestando que en base al principio de legalidad su reforma es muy conveniente. Adicionalmente a estas afirmaciones, con el estudio teórico, el sustento legal, el acopio de información de fuentes confiables, la recolección de datos y la presentación de los resultados de la investigación de campo; todos en conjunto arrojan como consecuencia al problema planteado en la presente investigación la necesidad de una reforma al Código Orgánico Integral Penal.

7.2. Contratación de la Hipótesis.

La hipótesis planteada en esta investigación, es la siguiente:

“La falta de tipificación del delito de Estafa informática en el Código Orgánico Integral Penal (COIP), no permite su juzgamiento dentro de los parámetros propios de las Tecnologías de la Información y la Comunicación, vulnerando el patrimonio de las personas”.

Esta hipótesis en la presente investigación fue comprobada inicialmente con el desarrollo del marco conceptual, seguido del marco doctrinario, con el marco jurídico y finalmente con el Derecho comparado elaborado con la comparación de legislaciones de otros países con ciertos avances jurídicos en estos temas más que nuestro país. Por otra parte de la comprobación de esta hipótesis se realizó con la examinación y análisis de la investigación de campo, a sus resultados obtenidos de las encuestas y entrevistas; en donde la mayoría de la población muestra considera que, la falta de tipificación del delito de estafa informática de manera autónoma en la

Legislación Penal, deja ciertas posibilidades a la vulneración del patrimonio de las personas víctimas de estas modalidades delincuenciales, y que en su defecto los sujetos activos no reciba la sanción adecuada a este tipo de delitos, dado que no puede actualmente juzgarse ese delito dentro de los parámetros correspondientes. Por tanto, es necesario destacar que mi hipótesis en su comprobación es positiva.

7.3 Fundamentación Jurídica para la Propuesta de Reforma Legal.

El Ecuador como un Estado Constitucional de Derechos y Justicia Social, persiguiendo una filosofía jurídica garantista que posiciona a la Constitución de la República, como una norma suprema ante cualquier otra del ordenamiento jurídico interno establecido para regir el país; en su cuerpo normativo se señala que; en el Artículo 66, inciso 26, se reconoce y garantiza el Derecho a la propiedad en todas sus formas, y el Derecho al acceso a la propiedad, entre otras medidas; lo que afianza la obligación del Estado de adoptar las medidas públicas necesarias para garantizar y proteger este derechos a las ciudadanos ecuatorianos reconocidos como sujetos de derechos.

Además, en el Artículo 75 se estipula que toda persona tiene Derecho al acceso gratuito a la justicia y a la tutela efectiva, imparcial y expedita de sus derechos e intereses, con sujeción a los principios de inmediación y celeridad; en ningún caso quedará en indefensión. El incumplimiento de las resoluciones judiciales será sancionado por la ley;

Es oportuno recurrir al Código Orgánico Integral Penal como el conjunto sistematizado de normas con la característica de ser normas punitivas, establece el procedimiento para el juzgamiento de las personas con estricta observancia del

Debido Proceso, los derechos y garantías dictados en la Constitución de la República y demás leyes conexas.

Con ello el Artículo 2 de la legislación penal, que versa sobre los principios generales afines al debido proceso dictaminando que en lo que se refiere a materia penal se aplican todos los principios que emanan de la Constitución de la República, de los instrumentos internacionales de Derechos Humanos y los desarrollados en este mismo código. En torno a estos principios existen unos fundamentales ligados al debido proceso penal detallados en el Artículo 5 y referente al inciso 1, puntualiza uno de los más importantes que es el principio de legalidad donde se manifiesta que no existirá una infracción penal sin ley anterior al hecho.

Es conveniente recurrir también al Artículo 13 del Código Orgánico Integral Penal, sobre las normas de interpretación el cual regula que las normas de este Código deberán interpretarse de conformidad a ciertas reglas como: 1. La interpretación en materia penal se realizará en el sentido que más se ajuste a la Constitución de la República de manera integral y a los instrumentos internacionales de derechos humanos. 2. Los tipos penales y las penas se interpretarán en forma estricta, esto es, respetando el sentido literal de la norma. 3. Queda prohibida la utilización de la analogía para crear infracciones penales, ampliar los límites de los presupuestos legales que permiten la aplicación de una sanción o medida cautelar o para establecer excepciones o restricciones de derechos.

En este sentido, considero que la ausencia de la tipificación del delito de estafa informática no está considerada dentro del Artículo 186, que hace alusión al delito de estafa común; por cuanto su ausencia conduce a los operadores de justicia a un error de adecuación al tipo penal. El articulado existente resulta ser insuficiente

jurídicamente y no se presta para analogías o interpretaciones afines a la estafa informática por cuanto por esta ausencia se estaría viendo vulnerados derechos de protección y seguridad que el Estado garantiza a sus ciudadanos y sus bienes.

8. Conclusiones.

Una vez desarrollado el presente trabajo de investigación, en su parte teórica como en el análisis de campo, referente al tema denominado: “La Falta de Tipificación del Delito de Estafa informática en el Código Orgánico Integral Penal (COIP), perjudica el Patrimonio de las personas” he considerado pertinente establecer las siguientes conclusiones:

- En la actualidad con los avances de la tecnología de la información y la comunicación, ha ido apareciendo nuevas formas para cometer ilícitos mediante la ingeniería social, engaños, utilización de métodos avanzados para el ingreso en sistemas informáticos, cuyo objetivo es el copiar, borrar, modificar, transferir información en pocos segundos logrando de esta forma que colapsen varios sistemas informáticos, como también afectar la privacidad de las personas ya que en algunas ocasiones estos datos obtenidos de manera ilegal se los pueden vender por grandes sumas de dinero o a su vez hacer uso en beneficio propio para sustraer grandes cantidades de dinero para si mismo.
- En nuestro país es difícil determinar un número exacto de casos de personas que hayan sido víctimas de estafa a través de medios informáticos, ya que la mayoría no las denuncian, o si la denuncian son adecuados a otro tipo penal, o a su vez la investigación se ve truncada, porque no existe equipo especializado para la investigación de este tipo de casos, y el que Ecuador no

sea parte de ningún convenio internacional para combatir delitos informáticos no le permite tener cooperación internacional para la solución de estos casos.

- Para se ejecute el delito de estafa informática necesariamente debe existir el componente humano, la manipulación de medios informáticos por parte del sujeto logrando que la víctima voluntariamente entregue datos confidenciales; caso contrario el acto cometido se subsumiría al delito de estafa común o a su vez en otro tipo de delito.
- Es necesario la tipificación del delito de estafa informática y sus modalidades en el Código Orgánico Integral Penal basado jurídicamente en el principio de legalidad y seguridad jurídica.
- Con la tipificación del delito de estafa informática y sus modalidades en el código integral penal se estaría previniendo, protegiendo, y cumpliendo con los derechos que se garantizan en relación a los ciudadanos y a su patrimonio.

9. Recomendaciones

Las recomendaciones que considero oportunas poner en conocimiento a fin de dar solución a la problemática planteada en la presente investigación son las siguientes:

- Que como nación nos unamos a convenios internacionales contra la cyber delincuencia, para tener una mayor cooperación internacional y a la vez capacitarnos de las nuevas modalidades delictivas que surgen del avance de la tecnología día a día.
- Que las carreras de Derecho de las Universidades del Ecuador incorporen en las líneas de investigación, que los avances tecnológicos han traído consigo

nuevas modalidades delictivas que superan hoy en día a la normativa para sancionarlas.

- Que los encargados de administrar Justicia, presten mucho cuidado y diligencia en aquellos procesos que se sustancian por motivos de delitos de estafa informática, con la finalidad de no caer en el error y adecuar el delito de estafa informática al delito de estafa común u otros similares.
- Que la Asamblea Nacional del Ecuador reforme el Código Orgánico Integral Penal donde se tipifique la estafa informática en el catálogo de delitos como un delito autónomo a la estafa común, considerando las modalidades de este tipo de estafa informática hasta hoy en día ya conocidas.

10. Propuesta Jurídica

REPÚBLICA DEL ECUADOR

ASAMBLEA NACIONAL



CONSIDERANDO:

Que, el Artículo 1, de la Constitución de la República establece que el Ecuador es un Estado Constitucional de Derechos y Justicia, por consecuencia es necesario implementar cambios en el ordenamiento jurídico nacional que responda al

cumplimiento de su más alto deber de respetar y hacer respetar los derechos garantizados por la Constitución.

Que, el Artículo 66, inciso 26 de la Constitución de la República del Ecuador reconoce el Derecho a la propiedad en todas sus formas, con función y responsabilidad social y ambiental. El Derecho al acceso a la propiedad se hará efectivo con la adopción de políticas públicas, entre otras medidas.

Que, la Constitución de la República en su Artículo 75, contempla que toda persona tiene Derecho al acceso gratuito a la justicia y a la tutela efectiva, imparcial y expedita de sus derechos e intereses, con sujeción a los principios de inmediación y celeridad; en ningún caso quedará en indefensión. El incumplimiento de las resoluciones judiciales será sancionado por la ley.

Que, el Artículo 169, de la Constitución de la República del Ecuador garantiza la aplicación del sistema procesal como un medio para la realización de la justicia con observancia a principios de uniformidad, eficacia e inmediación, haciendo efectivas las garantías del Debido Proceso.

Que, en el Artículo 321, de la Constitución de la República reconoce y garantiza el Derecho a la propiedad en sus formas pública, privada, comunitaria, estatal, asociativa, cooperativa, mixta, y que deberá cumplir su función social y ambiental.

Que, Artículo 424, primer inciso, ordena que la Constitución es la Norma Suprema del Estado y prevalece sobre cualquier otra del ordenamiento jurídico, y, por lo tanto, todas las normas de menor jerarquía deben mantener conformidad con las disposiciones constitucionales.

Que, el Código Orgánico Integral Penal, tiene por finalidad normar el poder punitivo, tipificar infracciones penales, establecer el procedimiento para el juzgamiento de las personas con estricta observancia del debido proceso, promover la rehabilitación social de las personas sentenciadas y la reparación integral de las víctimas.

Que, el Artículo 2, del Código Orgánico Integral Penal referente a los principios generales afines al debido proceso refiere que en materia penal se aplican todos los principios que emanan de la Constitución de la República, instrumentos internacionales de derechos humanos y los desarrollados en este mismo código.

Que, el Artículo 5, inciso 1, Código Orgánico Integral Penal, sobre el principio de legalidad manifiesta que no existirá una infracción penal sin una ley anterior al hecho.

Que, el Artículo 13, del Código Orgánico Integral Penal sobre las normas de interpretación establece: 1. La interpretación en materia penal se realizará en el sentido que más se ajuste a la Constitución de la República de manera integral y a los instrumentos internacionales de Derechos Humanos. 2. Los tipos penales y las penas se interpretarán en forma estricta, esto es, respetando el sentido literal de la norma. 3. Queda prohibida la utilización de la analogía para crear infracciones penales, ampliar los límites de los presupuestos legales que permiten la aplicación de una sanción o medida cautelar o para establecer excepciones o restricciones de derechos.

Que, la Constitución de la República del Ecuador, en el Artículo 132, regula que la Asamblea Nacional aprobará como leyes las normas generales de interés común. Las atribuciones de la Asamblea Nacional que no requieran de la expedición de una ley se ejercerán a través de acuerdos o resoluciones. Se requerirá de ley en los siguientes

casos: 1. Regular el ejercicio de los derechos y garantías constitucionales. 2. Tipificar infracciones y establecer las sanciones correspondientes. 3. Crear, modificar o suprimir tributos, sin menoscabo de las atribuciones que la Constitución confiere a los gobiernos autónomos descentralizados. 4. Atribuir deberes, responsabilidades y competencias a los gobiernos autónomos descentralizados. 5. Modificar la división político-administrativa del país, excepto en lo relativo a las parroquias. 6. Otorgar a los organismos públicos de control y regulación la facultad de expedir normas de carácter general en las materias propias de su competencia, sin que puedan alterar o innovar las disposiciones legales, lo que justifica la tipificación del delito de estafa informática en el Código Orgánico Integral Penal.

Que, la Constitución de la República del Ecuador, garantiza en su Artículo 66, inciso 19, el Derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección.

En uso de las atribuciones y de conformidad con el Artículo 120, numeral 6 de la Constitución de la República del Ecuador expide lo siguiente:

**LEY REFORMATORIA DEL CODIGO ORGÁNICO INTEGRAL PENAL
(COIP)**

Art1. Agréguese al Artículo 186, dos nuevos incisos luego del segundo inciso que digan:

1. A través del uso de tecnologías de la información y la comunicación fabricaren, introdujeren, poseyeren o facilitaren programas informáticos,

instrucciones falsas o fraudulentas específicamente destinados a la comisión de estafas por un beneficio económico en perjuicio ajeno.

2. Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

La presente ley entrará en vigencia a partir de su promulgación en el Registro Oficial.

Dado en el Distrito Metropolitano de San Francisco de Quito, en la sala de sesiones de la Asamblea Nacional del Ecuador, a los 9 días del mes de marzo del año dos mil veintiunos.

f) Presidente de la Asamblea Nacional del Ecuador. f) Secretario General.

11. Bibliografía

- Alemania, R. F. (31 de enero de 1998). Código Criminal, Reformado 2019. *Estafa por Computador*. Munich : Deutscher Taschenbuch Verlag .
- Antinori, N. E. (2006). *Conceptos Básicos de Derecho*. Argentina: Editorial de la Universidad del Aconcagua.
- Asua, L. J. (1970). *Tratado del Derecho Penal* (Vol. Tomo VII). Buenos Aires , Argentina: Losada S.A.
- Bankinter, S. d. (12 de septiembre de 2019). *Bankinter*. Obtenido de <https://blog.bankinter.com/economia/-/noticia/2017/4/17/quees-smishing-vishing-ciberseguridad-consejos>
- Beltrán, S., Hernández, I., & Carbajal , A. (2012). La Integración de Redes de Colaboración Entre Cuerpos Académicos. *Alternativas en Psicología*.
- Bernardo Lerner OMEBA. (1960). *Enciclopedia Jurídica OMEBA* (Vol. X). Argentina: Editorial Bibliografica Argentina.
- Blogspot, S/A. (2012). Tecnologías de la Información y la Comunicación, Clasificación de las Tics, [en línea]. Disponible en: <http://informacion-comunicacion3.blogspot.com/p/clasificacion-de-las-tics.html>
- Bolivia, O. d. (1 de septiembre de 2018). *Observatorio de Delitos Informáticos Bolivia* . Obtenido de <https://www.odibolivia.org/2018/09/01/fraude-estafa-informatica/>
- Cabero, J. (1998) Las aportaciones de las nuevas tecnologías a las instituciones de formación continuas: Reflexiones para comenzar el debate. <http://tecnologiaedu.us.es/bibliovir/pdf/85.pdf>.
- Camacho Losa. (1987). *El delito informático*. España, Madrid: Bosch.
- Caro, A. M. (30 de octubre de 2015). *Penal Conocimiento* . Obtenido de <http://noticias.juridicas.com/conocimiento/articulos-doctrinales/10617-estafa-informatica-el-denominado-phishing-y-la-conducta-del-ldquo%3Bmulero/>
- Carrara, (1980) Programa de Derecho Criminal. Parte Especial (Traducción J. Ortega Torres y J. Guerrero, Bogotá, 2000), Tomo IV, Editorial Jurídica Continental.
- Casanova, R. (1987). *Poder Informático y Seguridad Jurídica*, . Madrid: Fundesco.
- Castillo, M. C. (1989). *El Delito Informático*. Zaragoza: Facultad de Derecho de Zaragoza, Congreso sobre Derecho Informático.
- Castillo, R. C. (04 de julio de 2016). *Derecho Ecuador* . Obtenido de <https://www.derechoecuador.com/la-antijuricidad>

- Castro, L. (2015). *¿Qué es hacker?* about en español. s.pág. Online. Internet. Consultado: 1 febrero 2015. Recuperado de: <http://aprenderinternet.about.com/od/ConceptosBasico/g/Que-Es-Hacker.htm>
- Ciprian, R. (2010). *Tratado de Derecho Inmobiliario* (Tercera Edición ed.). Santo Domingo, República Dominicana.: V Centenario.
- Club Universitario Alicante (2010). *Delitos y Delincuentes*, España, Alicante.
- Cobo Romaní, J. C. (2011). El concepto de tecnologías de la información. Benchmarking sobre las definiciones de las TIC en la Sociedad del conocimiento . *Zer-Revista de Estudios de Comunicación*, 14, 295-318.
- COIP, M. d. (10 de febrero de Registro Oficial 180;2014). Código Orgánica Integral Penal. Quito, Ecuador : Gráficas Ayerve C.A.
- CRE, C. d. (20 de octubre de RO 449:2008). Constitución de la República del Ecuador CRE. Quito, Ecuador: Corporación de Estudios y Publicaciones.
- Cuadras, A. P. (11 de mayo de 2016). *blogspot.com*. Obtenido de Tecnologías de la Información y la Comunicación: <http://lasticspatricia.blogspot.com/2016/05/definicion-de-las-tics-segun-diversos.html>
- Cueva, A. J. (14 de julio de 2015). *Garberi Penal* . Obtenido de <http://www.garberipenal.com/3-tipos-de-estafas-comunes-a-traves-de-medios-informaticos/>
- Definiciona. (2019). *Definiciona* . Obtenido de concepto y etimología, falta: <https://definiciona.com/falta/#palabras-relacionadas>
- Definiciones-de.com. (15 de 09 de 2018). *Definiciones-de.com*. (ALEGSA, Editor) Obtenido de Definición de tipificar : <http://www.definiciones-de.com/Definicion/de/tipificar.php>
- Delito de Blanqueo de Capitales. Estafa Informática. Phishing. Claves de Acceso a Cuentas Bancaria, 2422/2011, Tribunal Supremo - Sala Segunda, de lo Penal 25 de octubre de 2012.
- Delito de Estafa , Sentencia 11090, Corte Suprema de Justicia de Colombia, M.P. Jorge Aníbal Gómez Gallego. 16 de julio de 2001.
- Díaz, W. D. (19 de enero de 2013). Hacia una reflexión histórica de las TIC. *Hallazgos*, 10, 213-233.
- Ecuador, A. (08 de 07 de 2019). *Abogados Ecuador*. Obtenido de <https://abogadosecuador.com.ec/post/delitos-informaticos-en-crecimiento>
- Egas, D. J. (2014). *Código Orgánico Integral Penal (COIP) Teoría del delito y sistema acusatorio*. (primera ed.). Perú: Murillo Editores.

- Europa, C. d. (23 de noviembre de 2001). Convenio sobre la Ciberdelincuencia . *Tratado Europeo No. 185*. Budapest.
- Félix, S. P. (14 de mayo de 2016). *blogspot.com*. Obtenido de Las TIC: <http://stefaniperezfelix.blogspot.com/2016/05/definicion-de-autores-de-las-tics.html>
- Fernandez, M. (23 de abril de 2019). *Secure and private email service*. Obtenido de <https://blog.mailfence.com/es/smishing/>
- FJ., R. D. (2009). *Tecnologías de la información y la comunicación y nuevas dimensiones de los derechos fundamentales*.
- Galán, J. S. (30 de enero de 2019). *Economipedia* . Obtenido de Patrimonio : <https://economipedia.com/definiciones/patrimonio.html>
- Gardey, J.P (2013) *Definición de Patrimonio*. <https://definición.de/patrimonio/>
- García, D, El Phishing como delito de estafa informática. Comentario a la SAP de Valencia, véase en: http://www.scielo.org/bo/pdf/rbd/n25/n25_a25.pdf
- Gorrín., A. H. (5 de diciembre de 2011). *economiat.com*. Obtenido de Concepto de TIC: Tecnologías de la Información y la Comunicación: <https://economiat.com/concepto-de-tic/>
- Huerta Miranda, M & Líbano, M.C, Los Delitos Informáticos, Editorial Jurídica Cono Sur.
- IgnotoAzaustre, M. J., Fernández Sánchez, C. M., Lucero Manresa, J. L., Navarro, E., & Ramos González, M. Á. (2001). *Peritajes Informáticos* . Madrid: Ediciones Díaz de Santos S.A. .
- Jimenez de Asua, L. (1970). *Tratado del Derecho Penal* (Vol. Tomo VII). Buenos Aires , Argentina: Losada S.A.
- Juridica, E. (Edición 2020). *Enciclopedia Juridica de Derecho* . Obtenido de <http://www.encyclopedia-juridica.com/d/derecho/derecho.htm>
- Kluwer, W. (s.f.). *Wolters Kluwer*. Obtenido de Derecho de Propiedad: https://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAAAAEAMtMSbF1jTAAAUMjYzMTtbLUouLM_DxbIwMDCwNzAwuQQGZapUt-ckhlQaptWmJOcSoAPeW7BjUAAAA=WKE
- Leys-0155 . (29 de octubre de 1921). *Codigo Penal De La Nación Argentina*. B.O. 03/11/1921.
- Liszt, F. V. (1944). *Tratado de Derecho Penal, versión española de la 20ª* (20 ed., Vol. II). Madrid.
- MAGLIONA MARKOVICTH Claudio Paúl, LÓPEZ MEDEL Macarena, *Delincuencia y Fraude Informático*, Editorial Jurídica de Chile. 1999

- MisAbogados.com. (04<https://www.misabogados.com.co/blog/que-es-una-estafa> de mayo de 2016). *MisAbogados.com*.
- Mok, S. C. (2010) *Privacidad Y Protección De Datos: Un Análisis De Legislación Comparad*. Dialogos, Revista Electrónica de Historia. Vol.11
- Moscoso, A. (2008). Las Tecnologías De La Información Y La Comunicación En La Formación Profesional. Andalucía, España: Revista Digital para profesionales de enseñanza.
- Muñoz, J.(2005) (s.f.). *Comentarios a la parte especial del derecho penal.España*: Editorial Aranzadi.
- Ottone, M & Hopenhayn M. (2000) Desafíos educativos ante la sociedad del conocimiento. Rev. Argentina: Pensamiento Educativo, Vol. 40, N° 1
- Penal, C. O. (10 de febrero de 2014). Código Organico Integral Penal . Quito , Quito, Ecuador: Gráficas Ayerve C.A.
- Penalistas, C. A. (s.f.). *Chabaneix* . Obtenido de Estafa: <https://chabaneixabogadospenalistas.es/derecho-penal-economico/estafa/>
- Peña, O. y Almanza, F. (2010). *Teoría del Delito Manual Práctico para su aplicación en la teoría del caso*. Lima, Perú: Editorial Nomos y Thesis E.I.R.L.
- Porto, J. P., & Gardey, A. (2009). *Definicion.de: Definición de falta*. Obtenido de <https://definicion.de/falta/>
- Porto, J. P., & Gardey, A. (2013). *Definicion.de*. Obtenido de Regulación: <https://definicion.de/regulacion/>
- Porto, J. P., & Merino, M. (2008. Actualizado: 2012.). *Definicion.de*. Obtenido de CONDUCTA: <https://definicion.de/conducta/>
- Quezada, C. M. (2010). La Evolución de las Tecnologías de la Información y Comunicación. *ACORDES*, 117-134.
- Raffino, M. E. (11 de octubre de 2019). *Concepto.de*. Obtenido de CONDUCTA : <https://concepto.de/conducta/>
- Raffino., M. E. (14 de enero de 2019). *Concepto.de*. Obtenido de "Derecho de propiedad": <https://concepto.de/derecho-de-propiedad/>.
- Real Academia Española RAE. (2014). *Diccionario de la Lengua Española* (23.^a edición ed., Vol. un volumen). Madrid: Espasa Libros, S. L. U.
- Real Academia Española RAE. (2016). *Gran Diccionario de la Lengua Española* . Madrid : Larousse Editorial, S.L.
- Real Academia Española RAE; Concejo General del Poder Judicial. (2016). *Diccionario del Español Juridico*. Madrid: S.L.U. ESPASA LIBROS.

- Regalado, J. H., & Cisneros, V. S. (2012). Tipificación de Infracciones Penales en materia de Propiedad Intelectual. Quito : Universidad de las Américas.
- Registro Oficial 46. (24 de junio de 2019). Código Civil . *ultima modificacion*. LEXIS FINDER.
- Roig, C. F. (2008). *Tecnología de la Información. Conceptos Básicos*. Mallorca : San José Obrero.
- Ron, A. M. (2019). *DerechoEcuador.com*. Obtenido de Estafa Informática: <https://www.derechoecuador.com/estafa-informatica>
- Roxin, C. (1997', Pag. 194-195). *Derecho Penal, Parte General, Parte I, Fundamentos. La Estructura de la Teoría del Delito*. Madrid, España: Editorial Civitas.
- Roxin, C. (2000). *Derecho Penal Parte General. Fundamentos. La Estructura de la Teoría del Delito*. Madrid : Editorial Civitas S. A. Segunda Edición.
- Roxin, C. (2002). *Política Criminal y Sistema de Derecho Penal* . Buenos Aires: Editorial Hammurabi .
- Orellana, W.O.A, (2004). *Teoría del Delito Sistemas Causalista, Finalista y Funcionalista*. D.F, México: Editorial Porrúa.
- Saín, G. R. (2012). Delito y nuevas tecnologías: fraude, narcotráfico y lavado de dinero por internet. Ciudad Autónoma de Buenos Aires: Del Puerto
- Seisdedos, P. S. (25 de marzo de 2018). *CogniFit*. Obtenido de conducta : <https://blog.cognifit.com/es/conducta/>
- Serralde, A (2010). *Clasificación de las tecnologías de la información y comunicación*, [en línea]. Disponible en: <http://es.slideshare.net/AleksNet/clasificacin-de-las-tics>
- Significados.com. (22 de octubre de 2018). Obtenido de "Derecho de propiedad": <https://www.significados.com/derecho-de-propiedad/>
- SCHNEIER. (01 de 09 de 2015). DELITOS INFORMÁTICOS. Recuperado el 10 de 07 de 2018, de PREZI: <https://prezi.com/nhbj6dbayaef/untitled-prezi/>
- Shutherland. E.(1939) Los Delitos de Cuello Blanco. Madrid. cuello
- Tecnología, B. M. (02 de agosto de 2017). *BBC Mundo* . Obtenido de <https://www.bbc.com/mundo/noticias-40802167>
- Torres, G. C. (2003). *Diccionario Jurídico Elemental* (Decimo séptima edición ed.). Argentina: Editorial Heliasta S.R.I.
- Trejo, M. A., Alvarez, G. A., & Chimbo., M. K. (2015). La seguridad Jurídica frente a los delitos informáticos. *Avances, Revista de Investigación Jurídica*, ISSN 2220-2129.

- Ucha, F. (abril de 2010). *Definición ABC*. Obtenido de <https://www.definicionabc.com/general/regulacion.php>
- UNAM, *Universidad Nacional Autónoma de México* (2018) Obtenido de <http://tutorial.cch.unam.mx/bloque4/lasTIC>
- Unesco. (2002). *Documents General Conference, Executive Board*,. Paris: Unesco.
- Valdes, J. T. (1966). *Los Delitos informáticos Situación en México” Informática y Derecho N° 9, 10 y 11, UNED*. Merida: UNED Centro Regional de Extremadura.
- Valdes, J. T. (1996). *Derecho Informático*. México: Mc. Graw Hill.
- Vasconcelos, F. P. (2009). *Derecho Penal Mexicano Parte Especial* (Vol. 1). México: Porrúa.
- Villalta, A. E. (2007). *La Privacidad y la Protección de Datos Personale*. Comité Jurídico Interamericano: O
- Welzel Hans, (1951), *La Teoría de la Acción Finalista, Buenos Aires, Argentina: Editorial Depalma*
- Yáñez, M. R., & Villatoro S, P. (2005). *Las Nuevas Tecnologías de la información y de la comunicación (TIC) y la Institucionalidad social. Hacia una Gestión Basada en el Conocimeinto* (Vol. Series CEPAL). Santiago de Chile: Naciones Unidas.
- Zambrano, R. (2012). *Delitos Contemplados en la Ley Ecuatoriana*. Quito: cecs.espol.
- Zarich, F. (2005). *Derecho Informatico 4*. República Argentina: Editrial Juris.

12. Anexos

12.1. Proyecto de Tesis



UNIVERSIDAD NACIONAL DE LOJA

Área Jurídica Social y Administrativa

CARRERA DE DERECHO

TEMA:

La Falta de Tipificación del Delito de Estafa informática en el Código Orgánico Integral Penal (COIP), perjudica el Patrimonio de las personas.

AUTORA:

Claudia Karina Medina González

DOCENTE:

Dr. Mario Sánchez

DIRECTORA:

Dra. Elena Carrión

LOJA-ECUADOR

2019-2020

1. TEMA

La Falta de Tipificación del Delito de Estafa Informática en el Código Orgánico Integral Penal (COIP), perjudica el Patrimonio de las personas.

2. PROBLEMATIZACIÓN

Las Tecnologías de la Información y la Comunicación hoy en día son de gran utilidad al permitir mantenernos comunicados, el comprar-vender productos, objetos y hasta información, compartir datos personales, el conversar e interactuar en tiempo real, la búsqueda de información, banca online, etc. Si bien es cierto, el uso de estas tecnologías facilita la vida de toda la sociedad, así mismo trae consigo desventajas, ya que el uso de las tecnologías de la información y la comunicación es libre, dá lugar a mejorar o crear nuevas formas de cometer conductas ilícitas por la cantidad de información personal que se sube al sin número de aplicaciones que la tecnología nos ofrece afectando de esta forma a sistemas y datos informáticos, secretos de comunicación, el patrimonio de las personas, la fe pública, la libertad sexual entre otros.

En nuestro país se encuentra tipificados delitos informáticos en nuestro Código Orgánico Integral Penal en los artículos 178, 190, 229, 230, 231, 232, 233, 234, y no se ha tomado en consideración las conductas de smishing, phishing y vishing que son propias de las Tecnologías de la Información y Comunicación TICs, como delitos de Estafa Informática, que comúnmente son confundidas con el delito de estafa común en el numeral 2 en el que específicamente hace referencia a la defraudación en dispositivos de uso bancario “cajero bancario”, pero no todos los tipos de defraudación informática son realizados por ese tipo de medios, tal es el caso de la programación de mensajes de texto, aplicaciones de mensajería (*smishing*) entre los más comunes WhatsApp, Messenger, Instagram, Facebook, entre otros, el uso de Sistemas de Comunicación confiables tales

como correos electrónicos (*pishing*) y a través de llamadas telefónicas (*vishing*), es decir, conductas antijurídicas cometidas mediante el uso de las tecnologías de la información y la comunicación, atentando contra el derecho a la propiedad constitucionalmente reconocida y afectando de esta forma a la sociedad en común y su patrimonio, al ser los usuarios víctimas directas de estas conductas que se ejecuta ilegalmente con fines de lucro.

El problema jurídico se produce al no encontrarse tipificadas las conductas *smishing*, *pishing* y *vishing* en el Código Orgánico Integral Penal como delitos de Estafa Informática, por cuanto el concepto de Estafa común que maneja nuestro Código Orgánico Integral Penal su verbo rector no alcanza a tipificar las características propias de lo que en derecho comparado e internacionalmente se está tipificando como estafa informática, que nace del avance y desarrollo de las Tecnologías de la Información y la Comunicación TICs, dejando en desventaja a la Legislación Penal Ecuatoriana para juzgar este tipo de conductas con sus particularidades propias del avance de las Tecnologías de la Información y la Comunicación TICs, concluyendo que existe un vacío legal al no haberse tipificado este tipo de conductas y por lo que es necesario, se incluya dentro del catálogo de delitos informáticos a la estafa informática y sus tres tipos de conductas antes singularizados, el mismo que me propongo desarrollar en este proyecto de tesis previo a mi graduación.

3. PROBLEMÁTICA

La falta de tipificación del delito de Estafa Informática en la legislación penal Ecuatoriana, por la introducción, alteración, borrado o supresión de datos informáticos; y la interferencia en el funcionamiento de sistemas informáticos con intención fraudulenta o delictiva para obtener ilegítimamente beneficio económico para sí o para otra persona causa daño patrimonial al titular de los datos o a terceros. Actualmente el Código Orgánico Integral Penal se limita a la estafa común sin tomar en cuenta el desarrollo de las Tecnologías de la Información y la Comunicación.

Síntesis: La falta de tipificación del delito de Estafa Informática en el Código Orgánico Integral Penal (COIP), causa daño patrimonial al titular de los datos o a terceros. Actualmente el Código Orgánico Integral Penal (COIP) se limita a la estafa común sin tomar en cuenta el desarrollo de las Tecnologías de la Información y la Comunicación.

4. JUSTIFICACIÓN

El uso de las tecnologías de la Información y la comunicación el avance y desarrollo de las mismas nos permiten estar comunicados e informados a nivel mundial en cuestión de segundos, pero así mismo trae consigo nuevas formas de delinquir debido a gran cantidad de información personal que se sube en diferentes aplicaciones que nos ofrece la tecnología, es por eso que me propongo realizar una investigación acerca de conductas antijurídicas que nacen del avance y desarrollo de las Tecnologías de la Información y la Comunicación TICs, como son la programación de mensajes de texto, aplicaciones de mensajería (smishing), el uso de Sistemas de Comunicación confiables tales como correos electrónicos (pishing) y llamadas telefónicas (vishing), y que dentro de nuestras leyes aun no se las han tipificado como tales, al no encontrarse tipificados los operadores de justicia juzgan a estas conductas como un delito de estafa común estipulado dentro de nuestro Código Integral Penal en su artículo 186, y por las características que poseen no caben dentro de este tipo penal, ya que por las características que poseen se trataría de un delito informático como es la estafa informática realizado mediante el uso de las Tecnologías de la Información y Comunicación TICs, es por ello que mi investigación se centrará en hacer una diferenciación tanto del delito de estafa común como de la estafa informática con sus características y elementos propios, para de esta forma proponer una reforma de creación de un tipo penal que se incluirá dentro de nuestras leyes para de esta forma facilitar su juzgamiento, así como la protección de la propiedad de la ciudadanía constitucionalmente reconocida, al permitir un juzgamiento adecuado y

dentro de los parámetros propios de las Tecnologías de la Información y la Comunicación TICs.

Considero que la investigación que realizaré contiene elementos de trascendencia social ya que los medios tecnológicos de uso común en toda la sociedad y que cualquier ciudadano común puede o fue víctima de una de estas conductas, de importancia jurídica ya que considero es importante que este tipo de delitos sean juzgados correctamente con las características propias de la estafa informática y con un propio tipo penal y es factible porque tendré la facilidad de acudir a profesionales entendidos en la materia para obtener información actualizada de registros de denuncias, casos así mismo a testimonios de víctimas de estos tipos de delitos.

5. OBJETIVOS

5.1 OBJETIVO GENERAL

- Realizar un estudio teórico, doctrinario y jurídico del delito de estafa para demostrar que la tipificación general del artículo 186 numeral 2 del Código Orgánico Integral Penal (COIP) no abarcan las conductas de estafa informática, y es necesario tipificarlas en la legislación penal ecuatoriana. Proponer reforma jurídica.

5.2 OBJETIVOS ESPECIFICOS

- Realizar un estudio teórico, normativo y doctrinario del delito de estafa para contrastar con el derecho comparado la nueva tipificación de la estafa informática en el desarrollo de las Tecnologías de la Información y la Comunicación que no se encuentra tipificado en el Código Orgánico Integral Penal (COIP).

- Determinar que existe confusión entre el delito de estafa común y estafa informática.

- Presentar propuesta de reforma al Código Orgánico Integral Penal (COIP), en el que se incorpore el delito de Estafa Informática.

6. HIPOTESIS

La falta de tipificación del delito de Estafa informática en el Código Orgánico Integral Penal (COIP), no permite su juzgamiento dentro de los parámetros propios de las Tecnologías de la Información y la Comunicación, vulnerando el patrimonio de las personas.

7. MARCO TEORICO

7.1 Tipificación

En la legislación penal definir una acción u omisión concretas, a las que se asigna una pena o sanción. (RAE, Diccionario de la Lengua Española, 2014).

La tipificación es la descripción de la materia de la prohibición, la realización del mismo es un indicio de la antijuridicidad de la acción". (Egas, 2014)

Es la criminalización de una norma de cultura realizada por el legislador y establecida por una ley penal, la descripción precisa de las acciones y omisiones que son consideradas como delitos y a los que se les asigna una pena o sanción. (Regalado & Cisneros, 2012)

Para el maestro Jiménez Huerta, "es la suma de aquellos elementos materiales que permiten establecer la esencia propia de un delito e integra el núcleo del concepto en torno al cual se agrupan los demás elementos" (Vasconcelos, 2009)

7.2 Delito

En palabras de Luis Jiménez de Asúa es toda acción u omisión o comisión por omisión típicamente antijurídica y correspondientemente imputable al culpable, siempre y cuando no surja una causal de exclusión de la pena o en el enjuiciable se susceptible de la aplicación de una medida de seguridad. (Asua, 1970)

Al criterio del Dr. Jorge Zavala Egas, quien dice que “El delito es una creación del hombre, es fruto de la cultura durante el desarrollo histórico de la convivencia humana y, por ello; el concepto puede variar en cada agrupación social y en cada momento distinto de la historia.” (Egas, 2014).

VON LISZT, sostiene que el delito es el comportamiento humano típicamente antijurídico y culpable, añadiéndose a menudo la exigencia que sea punible. (Liszt, 1944)

7.3 Estafa

Según el diccionario jurídico de la Real Academia Española estafa “es el delito que comete el que, con ánimo de lucro, utiliza engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno” (RAE, Diccionario del Español Jurídico, 2019).

Especie defraudación contra el patrimonio ajeno que en perjuicio del mismo tiene por objeto la obtención de un provecho injusto. (Bernardo Lerner OMEBA, 1960)

La estafa es una defraudación cometida mediante engaño apto para inducir en error. (Delito de Estafa , 2001)

7.4 Tecnologías de la Información y la Comunicación

Díaz define a las Tecnologías de la Información y la Comunicación como el conjunto de herramientas, soportes y canales desarrollados y sustentados por las tecnologías (telecomunicaciones, informática, programas, computadores e internet) que permiten la adquisición, producción, almacenamiento, tratamiento, comunicación, registro y presentación de informaciones, en forma de voz, imágenes y datos, contenidos en señales de naturaleza acústica, óptica o electromagnética a fin de mejorar la calidad de vida de las personas. (Díaz, 2013)

Así lo considera también Díaz Revorio cuando menciona que considera « como tecnologías de la información y de la comunicación o nuevas tecnologías, y entre otros instrumentos de transmisión y recepción de comunicaciones e informaciones, la telefonía fija, el móvil, la radio y la televisión, el GPS (Global Positioning System), la informática y los ordenadores, el fax, la videoconferencia, los SMS (Short Message Service) y otros

servicios de mensajería, el correo electrónico, el chat o mensajería instantánea, y ocupando un indiscutible protagonismo, Internet, que incluye hoy buena parte de las anteriores prestaciones”. (FJ., 2009)

Las Tecnologías de la Información y la Comunicación con el “conjunto de recursos necesarios para tratar información a través de ordenadores y dispositivos electrónicos, aplicaciones informáticas y redes necesarias para convertirla, almacenarla, administrarla y transmitirla. A nivel de usuario, sea individual o empresa, las TIC forman el conjunto de herramientas tecnológicas que permiten un mejor acceso y clasificación de la información como medio tecnológico para el desarrollo de su actividad”. (Gorrin., 2011)

7.5 Estafa Informática

Según el diccionario jurídico de la Real Academia estafa informática es “el delito de estafa que se comete por medios informáticos” (RAE, 2019)

CAMACHO LOSA presenta las notas del fraude informático 1.º una conducta fraudulenta (no profundiza en lo que deba entenderse por fraudulento), que consiste en un uso indebido o una manipulación fraudulenta de elementos informáticos; 2.º la presencia de los componentes físicos y / o lógicos del sistema informático como instrumento de auxilio de la conducta; 3.º la finalidad perseguida de obtener un beneficio ilícito (elemento

subjetivo que se concreta en el ánimo de lucro injusto); 4.º la producción de un perjuicio en otro. Este elemento aparece matizado por el propio autor al apuntar que puede no consistir en un perjuicio económico cuantificable. (Losa, 1987)

Por su parte, ROMEO CASABONA describe el fraude informático (que inicialmente denomina «manipulación de datos informatizados») como «la incorrecta modificación del resultado de un procesamiento automatizado de datos, mediante la alteración de los datos que se introducen o ya contenidos en el ordenador en cualquiera de las fases de su procesamiento o tratamiento informático, con ánimo de lucro y en perjuicio de tercero. (CASABONA, 1987)

Estafa informática es quien con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro ". (DELITO DE BLANQUEO DE CAPITALES. ESTAFA INFORMÁTICA. PHISHING. CLAVES DE ACCESO A CUENTAS BANCARIA, 2012)

porque el engaño ha creado un conocimiento deformado o inexacto de la realidad. Esto hace que la persona víctima del engaño actúe bajo una falsa presuposición de que la otra persona le ha manifestado la verdad.

Acto de disposición patrimonial: como consecuencia del engaño, que a su vez ha causado un error en la persona, tiene que producirse la entrega de un bien de forma voluntaria, que conlleva de forma directa la producción de un perjuicio patrimonial.

Ánimo de lucro: lo que quiere la persona que engaña es lograr un beneficio a costa de la persona engañada, por tanto el perjuicio que se causa a una y el beneficio que logra la otra están íntimamente relacionados. (Penalistas, s.f.)

8.4 Delitos Informáticos

Para Brooks delitos informático es cualquier acto ilegal para el que se precise un especial conocimiento de la tecnología de las computadoras, tanto para su realización como para su investigación y enjuiciamiento». (Brooks, 1983)

María Cinta Castillo entienden que "delito informático es toda acción dolosa que provoca un perjuicio a personas o entidades en cuya comisión intervienen dispositivos habitualmente utilizados en las actividades informáticas" (Castillo, 1989).

Los delitos informáticos son aquellas actividades ilícitas que: Se cometen mediante el uso de computadoras, sistemas informáticos u otros dispositivos de comunicación (la informática es el medio o instrumento para realizar un delito) tienen por objeto causar daños, provocar pérdidas o impedir el uso de sistemas informáticos (delitos informáticos). (Trejo, Alvarez, & Chimbo, 2015)

Julio Téllez Valdés conceptualiza al delito informático en forma típica y atípica, entendiendo por la primera a "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y por las segundas "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin" (Valdez, 1966)

8.4.1 Elementos para que se configure el delito de estafa informática

Para que existe el delito de estafa informática debe cumplir con los requisitos siguientes:

Obtener un resultado. - No necesariamente el resultado del acto debe ser falso, porque se puede obtener un resultado verdadero sin embargo lo podemos remplazar por otros datos, estos casos son comunes en los delitos de estafa informática en donde se obtiene un beneficio económico.

Datos. - Deberá tratarse de actos que manejen datos para lesionar el patrimonio del titular de los datos o de terceros, o a su vez, si se utiliza datos falsos. Los casos más comunes son en los delitos de phishing. De tal manera deberá realizarse la introducción, alteración, borrado o supresión de datos;

Tics. - El acto debe realizarse a través del uso de las Tecnologías de la Información y Comunicación, el mismo que deberá ser contado como inicio, medio y final;

Lucro. - Es importante señalar que en un delito de estafa siempre existirá un lucro, puesto que el delincuente busca ganancias pecuniarias, en la estafa informático, debe necesariamente un lucro, puesto que al no existir dicho tipo penal no se configurase y estaríamos hablando de sabotaje informático o acceso ilícito; y,

Bien Jurídico. - Debemos tener claro que bien jurídico tutela la estafa informática, puesto al existir las características antes señaladas, no se puede afirmar que este tipo penal

busca proteger la integridad de un sistema informático, de tal manera se tutela el funcionamiento del sistema informático. (Ron, 2019)

9. MARCO JURÍDICO

9.1 Protección al Derecho a la Propiedad en la Constitución de la República del Ecuador

La constitución de la Republica del Ecuador (CRE, RO 449:2018) en su Artículo 66 numeral 26 reconoce y garantiza a las personas; 26. El derecho a la propiedad en todas sus formas, con función y responsabilidad social y ambiental. El derecho al acceso a la propiedad se hará efectivo con la adopción de políticas públicas, entre otras medidas.

Además, en su artículo 321. El Estado reconoce y garantiza el derecho a la propiedad en sus formas pública, privada, comunitaria, estatal, asociativa, cooperativa, mixta, y que deberá cumplir su función social y ambiental

9.2 Patrimonio en la Constitución de la República del Ecuador

Art. 69.- Para proteger los derechos de las personas integrantes de la familia: 2. Se reconoce el patrimonio familiar inembargable en la cuantía y con las condiciones y limitaciones que establezca la ley. Se garantizará el derecho de testar y de heredar. (CRE, RO 449:2018)

9.3 Delito de Estafa en el Código Orgánico Integral Penal

Art. 186.- Estafa. (COIP, Registro Oficial 180;2014) La Persona que, para obtener un beneficio patrimonial para si misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que se realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años. La pena máxima se aplicará a la persona que:

1. Defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares.

Es con este artículo y numeral con el que se ha confundido las conductas antijurídicas de smishing, vishing y phishing, conductas realizadas mediante el uso de la Tecnologías de la Información y la Comunicación con el delito de estafa común.

9.4 Patrimonio en el Código Civil Ecuatoriano

El artículo 599 del Código Civil define la propiedad, señalando: El dominio que se llama también propiedad, es el derecho real de una cosa corporal, para gozar y disponer

de ella conforme a las disposiciones de las leyes y respetando el derecho ajeno, sea individual o social. (Registro Oficial 46, 2019)

9.5 Tipificación del delito de Estafa Informática en el Derecho

Comparado

El **Código Penal Español** en su Sección 1ª De las estafas, artículo 248. Establece que Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno. También se consideran reos de estafa: a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro. b) Los que fabricaren, introdujeran, poseyeran o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.

El Código Argentino en su artículo 172.- establece que será reprimido con prisión de un mes a seis años, el que defraudare a otro con nombre supuesto, calidad simulada, falsos títulos, influencia mentida, abuso de confianza o aparentando bienes, crédito, comisión, empresa o negociación o valiéndose de cualquier otro ardid o engaño. (LEYS-0155 , 1921)

El **Código Penal de Alemania** en su artículo 263a. establece el delito de Estafa por computador en los siguientes términos; (1) Quien con el propósito, de procurarse para sí o para un tercero una ventaja patrimonial antijurídica, en la medida en que él perjudique el patrimonio de otro, por una estructuración incorrecta del programa, por la utilización de datos incorrectos o incompletos, por el empleo no autorizado de datos, o de otra manera por medio de la influencia no autorizada en el desarrollo del proceso, será castigado con pena privativa de la libertad hasta cinco años o con multa. (Alemania, 1998)

El **convenio sobre Ciberdelincuencia** celebrado en Budapest el 23 de noviembre del 2001, con el objeto de proteger a la sociedad frente a la ciberdelincuencia en particular por los profundos cambios provocados por la digitalización, la convergencia y la globalización continua de las Tecnologías de la Información y la Comunicación y la información que éstas contienen, ponen en riesgo a la sociedad en general de ser víctimas de delitos informáticos entre estos el delito de estafa informática en su artículo 8 establece que “tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante: a.- cualquier introducción, alteración, borrado o supresión de datos informáticos; b.- cualquier interferencia en el funcionamiento de un sistema informático, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona” (Europa, 2001)

10.METODOLOGÍA

Para la planificación y ejecución de una investigación se requiere observar métodos, técnicas y procedimientos. La investigación que propongo y que ejecutaré observará los lineamientos institucionales previstos en el reglamento académico de la Universidad Nacional de Loja.

Entendido el método como el indicador del proceso investigativo que guiará la ejecución del proceso investigativo en la modalidad de tesis indico a continuación los métodos que utilizare y el modo en los que los aplicaré:

10.1 Método Inductivo

Propone el camino inverso: a partir de premisas particulares, se infieren conclusiones universales o generales, ya sea mediante inducciones completas (se consideran todos los elementos que integran el objeto de estudio) o incompletas (se consideran solamente algunos de los elementos que lo componen).

El mismo que me permitirá analizar casos o situaciones particulares de forma individualizada, partiendo desde el problema o tema planteado para mi investigación, y

de esta forma llegar a una conclusión general que me ayudará al descubrir temas generalizados del mismo: partiendo de una observación sistemática de la realidad. Parte de un análisis particular para llegar a lo general.

10.2 Método Deductivo

Se trata del método que parte de una hipótesis o explicación inicial, para luego obtener conclusiones particulares de ella, que luego serán a su vez comprobadas experimentalmente. Es decir, comprende un paso inicial de inferencias empíricas (observación, por ejemplo) que permiten deducir una hipótesis inicial que sea luego sometida a experimentación.

Este método me permitirá realizar un análisis partiendo desde un tema general hasta llegar a concluir en la situación del tema específico sobre el cual realizaré mi investigación, el mismo que me servirá para deducir un camino a tomar y de esta forma poder proponer una posible solución al tema investigado.

10.3 Método Analítico

El Método analítico es aquel método de investigación que consiste en la desmembración de un todo, descomponiéndolo en sus partes o elementos para observar

las causas, la naturaleza y los efectos. El análisis es la observación y examen de un hecho en particular. Es necesario conocer la naturaleza del fenómeno y objeto que se estudia para comprender su esencia. Este método nos permite conocer más del objeto de estudio, con lo cual se puede: explicar, hacer analogías, comprender mejor su comportamiento y establecer nuevas teorías.

A través de este método podré realizar un análisis de cada una de las categorías, secciones que conforman la totalidad de mi tema de investigación con mayor profundidad de forma separada, para de esta forma establecer o generar analogías y nuevas teorías para comprender conductas; así como el conocer a fondo el fenómeno de estudio.

En cuanto a las técnicas de investigación la técnica de la encuesta, entrevista, observación de campo y el fichaje.

10.4 Entrevista

Canales la define como "la comunicación interpersonal establecida entre el investigador y el sujeto de estudio, a fin de obtener respuestas verbales a las interrogantes planteadas sobre el problema propuesto, para obtener información útil para resolver la pregunta central de la investigación. A través de ella se obtiene información más completa

y profunda, además presenta la posibilidad de aclarar dudas durante el proceso, asegurando respuestas más útiles.

10.5 Encuesta

Las encuestas son un método de investigación y recopilación de datos utilizadas para obtener información de personas sobre diversos temas. Las encuestas tienen una variedad de propósitos y se pueden llevar a cabo de muchas maneras dependiendo de la metodología elegida y los objetivos que se deseen alcanzar. Implica solicitar a las personas información a través de un cuestionario, este puede distribuirse en papel aunque con la llegada de nuevas tecnologías es más común distribuir las utilizando medios digitales como redes sociales, correo electrónico, códigos QR o URLs.

La encuesta será aplicada a 30 abogados de libre ejercicio de su profesión: mientras que la entrevista la realizaré a profesionales involucrados con mi problematiza jurídica prefiriendo a aquellos que cuenten con posgrado en el área de conocimiento que investigo, docentes universitarios de la asignatura pertinente y autoridades relacionadas con mi problemática.

La metodología así indicada permitirá que la ejecución de la investigación se presente en la modalidad de tesis con los componentes: conceptual, doctrinario, jurídico, presentación y análisis obtenidos en la investigación de campo, conclusiones,

recomendaciones, fundamentación jurídica de la propuesta y mi propuesta de reforma e incorporación.

11.CRONOGRAMA

TIEMPO ACTIVIDADES		AÑO 2019 - 2020																															
		Octubre				Noviembre				Diciembre				Enero				Febrero				Marzo				Abril				Mayo			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Problematización	x	x																														
2	Elaboración de proyecto de tesis			x	x																												
3	Presentación y aprobación					x	X																										
4	Elaboración del Marco Conceptual							x	x																								
5	Elaboración del Marco Doctrinario									x	x																						
6	Elaboración del Marco Jurídico											x	x																				
7	Aplicación de la encuesta y entrevista													x	x																		
8	Análisis de Resultado de la investigación de campo															x	x																
9	Elaboración de conclusiones y recomendaciones																	x	x														
10	Elaboración de la propuesta de reforma																			x	x												
11	Presentación del informe final y primer borrador de tesis																					x	x										
12	Solicitud de tribunal de grado																							x	x								
13	Sustentación de tesis de grado final																									x	x	x					
14	Grado Oral																													x	x		

12.PRESUPUESTO Y FINANCIAMIENTO

12.1 Recursos Humanos

Director de Tesis: Por designarse

Autora: Claudia Karina Medina González

Población Investigada: Abogados de libre ejercicio, profesionales entrevistados.

12.2 Recursos Materiales

Nro.	Descripción	Valor
1	Computadora	680,00
2	Celular	380,00
3	Hojas de papel bon	20,00
4	Grabadora	60,00
5	Transporte	50,00
6	Copias	100,00
7	Impresiones	200,00
8	Materiales de oficina	90,00
9	Trabajo de campo	100,00
10	Empastado	90,00
11	Imprevistos	100,00
TOTAL		1870,00

El total de gastos asciende a MIL OCHOCIENTOS SETENTA DOLARES, que serán financiados con recursos económicos propios sin perjuicios de requerir un crédito educativo o ayuda económica de un centro de investigación o fundación

13. Bibliografía

(s.f.).

Alemania, R. F. (31 de enero de 1998). *Código Criminal, Reformado 2019. Estafa por Computador*. Munich : Deutscher Taschenbuch Verlag .

Antinori, N. E. (2006). *Conceptos Básicos de Derecho*. Argentina: Editorial de la Universidad del Aconcagua.

Asua, L. J. (1970). *Tratado del Derecho Penal* (Vol. Tomo VII). Buenos Aires , Argentina: Losada S.A.

Bankinter, S. d. (12 de septiembre de 2019). *Bankinter*. Obtenido de <https://blog.bankinter.com/economia/-/noticia/2017/4/17/quees-smishing-vishing-ciberseguridad-consejos>

Bernardo Lerner OMEBA. (1960). *Enciclopedia Jurídica OMEBA* (Vol. X). Argentina: Editorial Bibliográfica Argentina.

Bernardo Lerner OMEBA. (1966). *Enciclopedia Jurídica OMEBA* (Vol. XIV). Argentina: Editorial Bibliográfica Argentina.

Brooks, N. (1983). *Computer Crime: Prevention. Detection. Prosecution*. Neva York: Law and Business Inc. N.Y.

Caro, A. M. (30 de octubre de 2015). *Penal Conocimiento* . Obtenido de <http://noticias.juridicas.com/conocimiento/articulos-doctrinales/10617-estafa-informatica-el-denominado-phishing-y-la-conducta-del-ldquo%3Bmulero/>

CASABONA, R. (1987). *Poder Informático y Seguridad Jurídica*, . Madrid: Fundesco.

- Castillo, M. C. (1989). *El Delito Informático*. Zaragoza: Facultad de Derecho de Zaragoza, cingreso sobre Derecho Informatico.
- Ciprian, R. (2010). *Tratado de Derecho Inmobiliario* (Tercera Edición ed.). Santo Domingo , República Dominicana : V Centenario .
- COIP, M. d. (10 de febrero de Registro Oficial 180;2014). Código Orgánica Integral Penal. Quito, Ecuador : Gráficas Ayerve C.A.
- CRE, C. d. (20 de octubre de RO 449:2018). Constitución de la República del Ecuador CRE. Quito, Ecuador: Corporación de Estudios y Publicaciones.
- Cuadras, A. P. (11 de mayo de 2016). *blogspot.com*. Obtenido de Tecnologías de la Información y la Comunicación:
<http://lasticspatricia.blogspot.com/2016/05/definicion-de-las-tics-segun-diversos.html>
- Cueva, A. J. (14 de julio de 2015). *Garberi Penal* . Obtenido de
<http://www.garberipenal.com/3-tipos-de-estafas-comunes-a-traves-de-medios-informaticos/>
- Definiciones-de.com. (15 de 09 de 2018). *Definiciones-de.com*. (ALEGSA, Editor)
 Obtenido de Definición de tipificar : <http://www.definiciones-de.com/Definicion/de/tipificar.php>
- DELITO DE BLANQUEO DE CAPITALES. ESTAFA INFORMÁTICA. PHISHING. CLAVES DE ACCESO A CUENTAS BANCARIA, 2422/2011 (Tribunal Supremo - Sala Segunda, de lo Penal 25 de octubre de 2012).
- Delito de Estafa , Sentencia 11090 (Corte Suprema de Justicia de Colombia, M.P. Jorge Anibal Gómez Gallego. 16 de julio de 2001).

- Díaz, W. D. (19 de enero de 2013). Hacia una reflexión histórica de las TIC. *Hallazgos*, 10, 213-233.
- Ecuador, A. (08 de 07 de 2019). *Abogados Ecuador*. Obtenido de <https://abogadosecuador.com.ec/post/delitos-informaticos-en-crecimiento>
- Europa, C. d. (23 de noviembre de 2001). Convenio sobre la Ciberdelincuencia . *Tratado Europeo No. 185*. Budapest.
- Félix, S. P. (14 de mayo de 2016). *blogspot.com*. Obtenido de Las TIC: <http://stefaniperezfelix.blogspot.com/2016/05/definicion-de-autores-de-las-tics.html>
- Fernandez, M. (23 de abril de 2019). *Secure and private email service*. Obtenido de <https://blog.mailfence.com/es/smishing/>
- FJ., R. D. (2009). *Tecnologías de la información y la comunicación y nuevas dimensiones de los derechos fundamentales*.
- Galán, J. S. (30 de enero de 2019). *Economipedia* . Obtenido de Patrimonio : <https://economipedia.com/definiciones/patrimonio.html>
- Gardey., J. P. (2013). *Definicion.de*. Obtenido de Patrimonio: <https://definicion.de/patrimonio/>
- Gorrín., A. H. (5 de diciembre de 2011). *economiatric.com*. Obtenido de Concepto de TIC: Tecnologías de la Información y la Comunicación: <https://economiatric.com/concepto-de-tic/>
- Juridica, E. (EDICION 2020). *Enciclopedia Juridica de Derecho* . Obtenido de <http://www.encyclopedia-juridica.com/d/derecho/derecho.htm>

- Juridica, E. (Edición 2020). *EnciclopediaJuridica.com*. Obtenido de <http://www.encyclopedia-juridica.com/d/patrimonio/patrimonio.htm>
- Kluwer, W. (s.f.). *Wolters Kluwer*. Obtenido de Derecho de Propiedad: https://guiasjuridicas.wolterskluwer.es/Content/Documento.aspx?params=H4sIAAAAAAEAMtMSbF1jTAAAUMjYzMTtbLUouLM_DxbIwMDCwNzAwuQQGZapUt-ckhlQaptWmJOcSoAPeW7BjUAAAA=WKE
- LEYS-0155 . (29 de octubre de 1921). *CODIGO PENAL DE LA NACIÓN ARGENTINA*. B.O. 03/11/1921.
- Losa, C. (1987). *El delito informático*. Madrid: Bosch.
- México, U. N. (2018). *UNAM, Universidad Nacional Autónoma de México*. Obtenido de <http://tutorial.cch.unam.mx/bloque4/lasTIC>
- MisAbogados.com. (04<https://www.misabogados.com.co/blog/que-es-una-estafa> de mayo de 2016). *MisAbogados.com*.
- Penal, C. O. (10 de febrero de 2014). *Código Orgánico Integral Penal* . Quito , Quito, Ecuador: Gráficas Ayerve C.A.
- Penalistas, C. A. (s.f.). *Chabaneix* . Obtenido de Estafa: <https://chabaneixabogadospenalistas.es/derecho-penal-economico/estafa/>
- RAE, R. A. (2014). *Diccionario de la Lengua Española* (23.ª ed., Vol. un). Madrid, España: Espasa Libros S.L.U.
- RAE, R. A. (2019). *Diccionario del Español Jurídico*. Obtenido de <https://dej.rae.es/lema/estafa>

- Raffino., M. E. (14 de enero de 2019). *Concepto.de*. Obtenido de "Derecho de propiedad": <https://concepto.de/derecho-de-propiedad/>.
- Registro Oficial 46. (24 de junio de 2019). Código Civil . *ultima modificacion*. LEXIS FINDER.
- Ron, A. M. (2019). *DerechoEcuador.com*. Obtenido de Estafa Informatica: <https://www.derechoecuador.com/estafa-informatica>
- S/A. (2012). *Blogspot*. Obtenido de Clasificación de las TIC's: <http://informacion-comunicacion3.blogspot.com/p/clasificacion-de-las-tics.html>
- Significados.com. (22 de octubre de 2018). Obtenido de "Derecho de propiedad": <https://www.significados.com/derecho-de-propiedad/>
- Significados.com. (04 de marzo de 2018). *Significados.com*. Obtenido de Propiedad: <https://www.significados.com/propiedad/>
- Tecnología, B. M. (02 de agosto de 2017). *BBC Mundo* . Obtenido de <https://www.bbc.com/mundo/noticias-40802167>
- Torres, G. C. (2003). *Diccionario Jurídico Elemental* (Decimo séptima edición ed.). Argentina: Editorial Heliasta S.R.I.
- Trejo, M. C., Alvarez, G. A., & Chimbo, M. K. (2015). La Seguridad Jurídica frente a los Delitos Informaticos. *Avances, Revista de Investigación Jurídica* , ISSN 2220-2129.
- Valdez, J. T. (1966). *Los Delitos Informáticos. Situación en Mexico "Informática y Derecho No. 9, 10 y 11 UNED"*. Merida : UNED Centro Regional de Extremadura.

Sain , G. R. (2012). Delito y nuevas tecnologías: fraude, narcotráfico y lavado de dinero por internet . Ciudad Autónoma de Buenos Aires : Del Puerto .

García García Diego, El phishing como delito de estafa informática. Comentario a la SAP de Valencia, véase en: http://www.scielo.org.bo/pdf/rbd/n25/n25_a25.pdf

HUERTA MIRANDA, Marcelo y LÍBANO MANZUR Claudio, Los Delitos Informáticos, Editorial Jurídica Cono Sur.



.....
Claudia Karina Medina González
1900663970

12.2. Encuesta

UNIVERSIDAD NACIONAL DE LOJA. FACULTAD JÚRIDICA, SOCIAL Y ADMINISTRATIVA. CARRERA DE DERECHO

Abogado (a): Con el propósito de obtener datos que sustenten mi trabajo de investigación realizado bajo el tema “LA FALTA DE TIPIFICACIÓN DEL DELITO DE ESTAFA INFORMÁTICA EN EL CÓDIGO ORGÁNICO INTEGRAL PENAL (COIP), PERJUDICA EL PATRIMONIO DE LAS PERSONAS”, respetuosamente solicito a Usted se digne contestar la siguiente encuesta:

ENCUESTA.

Pregunta 1: ¿Conoce usted el delito de estafa común?

Pregunta 2: ¿Tiene conocimiento usted si en el Ecuador está tipificado el delito de estafa informática?

Pregunta 3: ¿Considera usted que existen diferencias entre el delito de estafa común y estafa informática? ¿Cuáles?

Pregunta 4: ¿Cree que es necesario tipificar en el Código Orgánico Integral Penal como delito autónomo a la estafa informática y sus modalidades?-La inserción de enlaces fraudulentos en redes sociales y correos electrónicos por parte del estafador, para obtener información personal y confidencial denominada **Phishing**, - La inserción de enlaces o mensajes fraudulentos a través de la telefonía móvil, para obtener información personal y confidencial, sea a través de mensajes de texto o WhatsApp denominado **Smishing**; y, -Las llamadas programadas de forma simultáneas a diferentes números mediante el cual obliga al usuario a llamar al número asignado so pena de ver perjudicado su patrimonio en su cuenta bancaria denominada **Vishing**, toda la información obtenida por el estafador es insertada por la víctima de forma voluntaria.

Pregunta 5: ¿Considera usted que al tipificar las modalidades de estafa informática en el Código Orgánico Integral Penal ecuatoriano se protegería el patrimonio de los ciudadanos?

12.3. Entrevista

UNIVERSIDAD NACIONAL DE LOJA. FACULTAD JÚRIDICA, SOCIAL Y ADMINISTRATIVA. CARRERA DE DERECHO

Abogado (a): Con el propósito de obtener datos que sustenten mi trabajo de investigación realizado bajo el tema “LA FALTA DE TIPIFICACIÓN DEL DELITO DE ESTAFA INFORMÁTICA EN EL CÓDIGO ORGÁNICO INTEGRAL PENAL (COIP), PERJUDICA EL PATRIMONIO DE LAS PERSONAS”, respetuosamente solicito a Usted se digne contestar la siguiente entrevista:

Pregunta 1

Con los elementos fundamentales que configuran el delito de Estafa Común tipificado en el art. 186 del Código Orgánico Integral Penal y los elementos que en doctrina señala como indispensables para que exista estafa informática encontrándose este último no tipificado en el Código Orgánico Integral Penal ¿Considera Ud. que hay diferencias entre estos dos tipos de estafa?

Estafa Común:

El delito de Estafa Común tipificada en el Artículo 186 del Código Orgánico Integral Penal producido por parte del estafador hacia la víctima presenta aspectos fundamentales como es el engaño, el daño al bien patrimonial y *específicamente en numeral 2 del mismo se limita solo a la alteración, clonación, adulteración o modificación de dispositivos originales de cajeros bancarios.*

Estafa Informática

Presenta los siguientes aspectos: a.- Manipulación fraudulenta de los elementos informáticos, b.- Presencia de sistemas informáticos, c.- Obtención de beneficio ilícito; y, d.- Perjuicio económico no cuantificable.

¿Por qué? Argumente su respuesta:

Tomando en cuenta que para cualquier modalidad de estafa es necesario que exista el engaño, considera usted que ¿Se podría argumentar que es debido a un error en virtud de, que la computadora o el medio electrónico indujo a el error?

Pregunta 2

En la doctrina, en fuentes informáticas y en algunas legislaciones extranjeras la estafa informática presenta las siguientes modalidades:

Phishing. - Es la inserción de un link fraudulento en redes sociales y e-mail por parte del estafador, para obtener información personal y confidencial, insertada por la víctima de forma voluntaria.

Smishing. - Es la inserción de enlaces o mensajes fraudulentos a través de la telefonía móvil, para obtener información personal y confidencial, ingresada por la víctima ya sea a través de mensajes de texto o aplicaciones de intercambio de textos como WhatsApp.

Vishing. - Son llamadas programadas de forma simultáneas a diferentes números mediante el cual obliga al usuario a llamar al número asignado so pena de ver perjudicado su patrimonio en su cuenta bancaria.

Como elemento importante es de resaltar que estas modalidades de DELITO NO SE ENCUENTRAN TIPIFICADOS EN EL CÓDIGO ORGÁNICO INTEGRAL PENAL, la Estafa Común tipificada en el Código Orgánico Integral Penal en el Artículo 186 es general que solo consta de dos elementos engaño, daño patrimonial, y *específicamente en numeral 2 del mismo se limita solo a la alteración, clonación, adulteración o modificación de dispositivos originales de cajeros bancarios.* Con estos elementos anotados apelo a su criterio especializado para que digno en argumentar, si usted ¿considera necesario el que se implemente en el Código Orgánico Integral Penal el delito de Estafa Informática y sus modalidades que son consecuencia de los avances científicos y tecnológicos?

Usted dentro de su carrera y experiencia profesional como abogado de libre ejercicio ¿ha tenido casos de este tipo de estafa?

Pregunta 3

Con los elementos antes mencionados ¿considera usted que para que se genere el delito de Estafa Informática es indispensable la manipulación de los dispositivos tecnológicos (hardware y software)?

Pregunta 4

¿Considera usted que, con el avance de las Tecnologías de la Información y la Comunicación, el delito de estafa común tipificado en el Código Orgánico Integral Penal no abarca lo que en su totalidad constituye la Estafa Informática?

Pregunta 5

¿Según su criterio profesional, se debería tipificar en el Código Orgánico Integral Penal el delito de Estafa Informática como delito autónomo, por tener elementos propios que no se subsumen en el delito de Estafa Común?
