Universidad del Azuay

Facultad de Ciencias Jurídicas

Carrera de Derecho

DELITO DE APROPIACIÓN FRAUDULENTA POR MEDIOS ELECTRÓNICOS BAJO LA MODALIDAD DE PHISING DENTRO DEL MARCO JURÍDICO ECUATORIANO

Autor:

María Paula Sempertegui Torres

Director:

Dr. Juan Carlos López

Cuenca – Ecuador

2022

DEDICATORIA

El presente trabajo de titulación se lo dedico a la memoria de mi padre Diego, y mi abuelo Hernán, quienes fueron mis mentores de vida y me alentaron a siempre cumplir con mis metas, obrando por el camino de la verdad.

AGRADECIMIENTO

Quiero agradecer a mis abuelos Primavera y Juan, por su guía y apoyo incondicional en el desarrollo de mi carrera universitaria.

A mi familia de sangre, mi madre Verónica, mis hermanos José Ignacio y Mariángel por su paciencia y comprensión infimita, a mis hermanos del alma; Eduardo, Soledad, Jorge y Juan Nicolas por hacer de mi carrera universitaria los mejores años de mi vida, gracias por su lealtad y sinceridad.

Un agradecimiento especial a la Universidad del Azuay, por abrirme sus puertas y formarme como profesional, a mis profesores por sus enseñanzas y el aprendizaje brindado.

Agradezco infinitamente a mi director del trabajo de titulación al Dr. Juan Carlos López quien ha sabido guiarme correctamente y ayudarme en todo lo necesario para la culminación de mi carrera.

RESUMEN

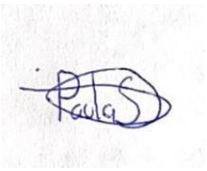
Mediante el presente trabajo investigativo, se pretende destacar la importancia del Delitos informático: apropiación ilegitima por medios electrónicos bajo la modalidad de phishing, determinado su alcance, regulación y fundamento jurídico, permitiendo así la visualización de los resultados ante la falencia e indebida aplicación derivan de la limitada regulación de estos delitos, a diferencia de legislaciones han optado por una normativa rigurosa al sancionar este tipo de conductas delictivas. De igual modo, se presentan criterios manifestados por doctrinarios del derecho, quienes exponen diversos puntos, sobre las medidas, desarrollo, y resultados en cuanto a la realidad actual, de la regulación de delitos informáticos.

ABSTRACT

This research work intended to highlight the importance of computer crime: illegitimate appropriation by electronic means under the modality of phishing. It was intended to determine its scope, regulation, and the legal basis. The results show the lack and improper application derived from the limited regulation of these crimes, unlike legislations that have chosen for a rigorous regulation to punish this type of criminal conduct. Similarly, criteria expressed by legal doctrinarians were presented, who exposevarious points on the measures, development, and results in terms of the current reality of the regulation of computer crimes.

Key words: crimes, legal property, fraud, computer crimes, phishing, electronic media, regulation, legal system.

Translated by



Paula Sempertegui

INDICE

Capítulo 1: Análisis los delitos informáticos Y sus generalidades.

1. Antecedentes Históricos de los Delitos informáticos

La creación de nuevas tecnologías, transacciones comerciales, la comunicación, los procesos industriales, las investigaciones, la seguridad, la sanidad, etc, son aspectos que dependen cada día más de un adecuado desarrollo de la tecnología informática.

Dada la extensión del uso de los ordenadores y de las redes de transmisión de datos en la mayoría de los ámbitos de nuestra sociedad, prácticamente todos los delitos pueden cometerse a través de un sistema informático; en este sentido, las conductas ilícitas vinculadas con los sistemas informáticos son muchas y heterogéneas.

La doctrina establece que: "El aspecto más importante de la informática radica en que la información ha pasado a convertirse en un valor económico de primera magnitud. Desde siempre el hombre ha buscado guardar información relevante para usarla después". (Magliona Markovicth y López Medel, 1999, p. 163). Existe un consenso general entre los diversos estudiosos de la materia, en considerar que el nacimiento de esta clase de criminalidad se encuentra íntimamente asociada al desarrollo tecnológico informático. Las computadoras han sido utilizadas para muchas clases de crímenes, incluyendo fraude, robo, espionaje, sabotaje y hasta asesinato. Los primeros casos fueron reportados en 1958. Para el profesor Mohrenschlager (1992) este fenómeno ha obligado al surgimiento de medidas legislativo penales en los Estados Industriales donde hay conciencia de que, en los últimos años, ha estado presente el fenómeno delictivo informático.

Los antecedentes de los delitos informáticos se sitúan a la par con el avance de la tecnología informática y la evidente influencia en gran parte de las áreas sociales,

pues, en virtud del desarrollo acelerado y mal uso de esta, ha surgido, por desgracia, comportamientos ilícitos que afectan la vida en comunidad.

A lo largo de la historia, hemos sido parte de diversos cambios particulares que diversifican una etapa de otra, es así como, el origen de los delitos informáticos puede situarse a partir de los años sesenta, en el cual el escenario literario infundía preocupación y temor en los ciudadanos por el almacenamiento y procesamiento de datos personales en ordenadores.

Ya en los años setenta, con la llegada de la difusión de los ordenadores, da lugar a las primeras manifestaciones de delincuencia informática en el desarrollo de las empresas, afectando de forma directa la economía de las mismas, provocando perdidas pecuniarias elevadas para el sector privado y público, a través de conductas como el fraude, sabotaje, manipulación y espionaje, conductas que se adecuan en el concepto inicial de delito informático, de modo que, a finales de la década de los 70, surgen los fraudes financieros en Estados Unidos producto de fallos en los sistemas de seguridad que carecían de protección adecuado a consecuencia de la inexperiencia de quienes en su momento administraban dichos sistemas.

Posteriormente, en los años ochenta, del incremento del uso de dispositivos electrónicos surge la piratería del software como infracción a la propiedad intelectual, misma que se intensificó a inicios de los noventa extendiéndose a productos como películas, música o videos juegos, los fraudes que se realizaban a través de la manipulación de uso de tarjetas de débito en cajeros automáticos, antecedentes que dieron lugar al tratamiento de estas problemáticas por los Organismos Internacionales.

Es así como, a finales de la década, se evidenció contenido ilícito en redes como amenazas, intercambio de pornografía infantil, actos que incitaban al odio, violencia y racismo por grupos extremistas, así como técnicas de hacking que alteraban y

manipulaban los sistemas gubernamentales, bancarios y de salud.

Por la propia naturaleza de Internet, permite que la información se encuentre al alance del público en general, además, se ha convertido en el medio adecuado para, educación, comercio, recreación, todo bajo un principio universal aceptado por quienes dan uso de la web, y que, por tanto, se vuelve un espacio que carece de regulación y por ente protección.

El Internet, se convirtió en una herramienta de simple uso y acceso, motivo por el cual, a consecuencia de la indebida utilización que puede otorgarse al mismo, ha dado lugar a una serie de actos ilícitos que actualmente se conocen comúnmente como delitos informáticos. En tiempos presentes, la incidencia del uso de los sistemas informáticos en todo ámbito, ha dado cabida a que cualquier delito pueda materializarse mediante el uso indebido las nuevas tecnologías de la información y de la comunicación.

En definitiva, la informática en un inicio se consideraba como un servicio con fines idóneos para el desarrollo de la sociedad, no obstante, con el trascurso del tiempo, el uso de medios electrónicos, dio lugar a ciertas conductas delictivas. Es así como, el avance tecnológico ha posibilitado la comisión de acciones delictivas que ponen en tela de duda la seguridad jurídica de los ordenamientos legales, puesto que los mismos no cuentan con los mecanismos adecuados para su investigación y juzgamiento, ya que, por la naturaleza digital de los crímenes, presentan un alta complejidad para el marco normativo de los Estados.

2. Definición y Características del Delito Informático.

La transformación tecnológica ha cumplido un papel indispensable en el desarrollo de la sociedad de la información y el acoplamiento del sistema social al

ecosistema digital, permitiendo así, la adhesión al ordenamiento jurídico de normas que regulen las nuevas modalidades de conductas delictuales. Los delincuentes han encontrado en la red, el camino idóneo para para revitalizar las estafas tradicionales, por lo que, siendo el Derecho un instrumento regulador por excelencia de las actividades sociales, no debe mantenerse al margen ni realizar una negación de este fenómeno, a pensar de la complejidad en lo que respecta a la carga probatoria, volviendo su comprobación de alta dificultad.

Una de las características fundamentales del mundo electrónico actual es su velocidad de evolución, actualmente se puede evidenciar nuevas formas de delincuencia informática, por cuanto, surge la importancia de limitar el uso inadecuado de medios informáticos, para evitar perjuicios en la vida económica de los ciudadanos, y así impedir la incidencia en la vida delictual, para así poder establecer con claridad cuáles son los medios utilizados, cuál es el daño causado, en qué campo interfiere, cuál es la conducta típica, y fundamentalmente si realmente existe una norma legal que tipifique estas conductas.

Se puede decir que la primera dificultad al momento de analizar los delitos informáticos, parte de propia conceptualización, es decir, que se puede entender por delito informático y que conductas se puede incluir en el mismo. A pesar de que no existe unanimidad en la doctrina, respecto a qué se entiende por Delincuencia Informática, es preciso el establecimiento de alguna definición.

Entonces, se puede definir al delito como:

La conducta (acción u omisión) típica, antijurídica, culpable y punible. Esta definición tiene carácter secuencial, es decir, el peso de la imputación va aumentando a medida que se pasa de una categoría a otra (de la tipicidad a la antijuricidad, de la antijuricidad a la culpabilidad, etc.), teniendo, por tanto, que

tratarse en cada categoría los problemas que son propios de la misma. (Conde, 2010, p. 45).

Una de las primeras definiciones fue la aportada por PARKER, que definió los abusos informáticos como "cualquier incidente asociado con la tecnología de los ordenadores en el que la víctima sufrió o pudo haber sufrido un daño y el autor, intencionadamente, obtuvo o pudo haber obtenido un beneficio". (Parker, citado por Diaz, 2009, p.23)

En este sentido, el concepto anteriormente desarrollado por el doctrinario, quien usa la expresión "forma abusiva del empleo de herramientas informáticas" da lugar a una definición extensa en relación con la noción tradicional de delito informático, conocida como aquella conducta delictiva cometido mediante el uso de la computadora u otro medio similar.

Julio Téllez-Valdés, en su libro Derecho Informático, enfoca el delito informático desde el punto de vista típico y atípico y lo define como "actitud contraria a los intereses de las personas en que se tiene a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tiene a las computadoras como instrumento o fin (concepto típico)'' (Téllez-Valdés, 2008, p.35).

Este enfoque doctrinal señala que el delito informático, más que una forma específica de delito, teniendo en cuenta que para su consideración, de igual forma debe cumplir con los elementos del delito, siendo estos: un acto típico, antijurídico, imputable y culpable sancionado por una pena, empero su distinción se da en la pluralidad de modalidades delictivas vinculadas, pudiendo ser los computadores, recursos electrónicos y cibernéticos, sin embargo, es pertinente mencionar que lo anteriormente expuesto, son los componentes y características, no independientes, que constituyen el concepto del delito.

Davara Rodríguez define al Delito informático como, ‘’la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software’’ (Davara Rodríguez, citado por Acurio, 2016, p.10).

Es así como, se evidencia desde diversos enfoques doctrinarios que determinan que el delito informático, más que considerarse una forma específica de delito, supone una pluralidad de modalidades delictivas vinculadas a dispositivos electrónicos como medio de ejecución de la conducta punible, razón por la cual, no es pertinente para su estudio, una individualización de los delitos informáticos, al contrario, es necesario realizar las modificaciones legales adecuadas a fin de adecuar los tipos tradicionales a la realidad social de momento.

Los autores Marcelo Huerta y Claudio Líbano definen los delitos informáticos como:

> Todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual, generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro. (Huerta y Líbano, 1966, p. 17)

En definitiva, es pertinente conceptualizar brevemente al delito informático como todo acto o conducta penalmente relevante que ostente la finalidad de causar lesión o puesta en peligro a un bien jurídico protegido mediante el uso de instrumentos

electrónicos, digitales e informáticos. Por cuanto, en concordancia a la doctrina, se puede definir al delito informático como la acción que reúne las características propiamente del delito, es decir que sea un acto típico, antijuridico, culpable, atribuible a su autor, empero, para su debida consideración, se requiere la implementación de un elemento informático o telemático al momento de su comisión, el cual es un presupuesto condicionante o necesario que permite que el justiciable cumpla con el objetivo de causar daño a bienes jurídicos protegidos, derechos y garantías reconocidos dentro del ordenamiento jurídico y que, son susceptibles de ser sancionadas por el Derecho Penal.

Una vez desarrollados los conceptos doctrinales de los delitos informáticos, es procedente traer a consideración las particularidades que caracterizan los mismos para un mejor entendimiento en su estudio. Cabe mencionar, que, a diferencia de cualquier hecho ilícito, que bien puede ser ejecutado por cualquier sujeto, los delitos informáticos, por el contrario, requieren de la participación de quien tenga un conocimiento avanzado en uso de medios electrónicos, por cuanto son consideradas conductas criminales de "cuello blanco".

Entre las características que presenta el delito informático, se considera la rapidez de su comisión, la distancia que puede existir entre el lugar de realización de la acción ilícita y el de la producción del resultado; así como, la dificultad para descubrir a sus autores quienes además tienen la facilidad de borrar las huellas o alterar programas y datos sin dejar rastro, asegurando su impunidad.

De igual forma, una de las características más relevantes en los delitos en cuestión, es la facilidad de tiempo y espacio, pues, para su consumación no es necesario un espacio físico, dificultado la comprobación de dicho hecho ilícito. Finalmente, suelen generar pérdidas económicas irremediables, de manera común a

instituciones financieras y sus usuarios que hacen uso de sus plataformas digitales.

Lo expresado es un punto importante, pues, como se puede apreciar, quienes cometen este tipo de ilícitos, tiene un amplio conocimiento en ciencias de la computación, e incluso, en ciertos casos, se encuentra posicionados en circunstancias que le permiten acceder a información de carácter sensible, causando un perjuicio económico en la mayoría de los casos. Frente a lo expresado, es común que estas conductas no lleguen a ser investigadas, o peor aún, no se pongan en conocimiento de la autoridad competente, esto en cuanto al alto índice de impunidad que existe en estos casos a causa de la falta de normativa que sancione estas actividades.

3. Incidencia de los Delitos Informáticos en la sociedad actual.

Bien se puede decir, que, uno de los cambios más importantes que se introdujo de la mano de las nuevas tecnologías, se suscita en la revolución industrial del siglo XIX, al sustituir el trabajo físico por maquinarias, evitando a los individuos la ejecución de ciertas tareas mecánicas tediosas y complejas.

Por cuanto, el avance informático ha sido beneficioso para la satisfacción del ser humano en diversos ámbitos como social, laboral, económico, entre otros, empero, dicho desarrollo, ha dado lugar al cometimiento de nuevos delitos, situando al derecho penal ante la problemática de abordar los mismos.

Actualmente, las nuevas tecnologías forman parte de todo ámbito de la vida diaria, presentando tanto ventajas, como desventajas que devengan de su mal uso, como es el aparecimiento de criminalidad informática, generando nuevas posibilidades de delincuencia.

Dentro de las formas comunes para la comisión de delitos informáticos suelen

ser el espionaje, fraude, robo, sabotaje, acoso, calumnias, injurias, acceso no autorizado a servicios informáticos, entre otros, mediante los cuales, se posibilita la vulneración de derechos, así como perjuicio a importantes bienes jurídicos materiales o morales.

En efecto, el incremento tecnológico, han generado herramientas para realizar actividades de gran relevancia social, como lo es la comunicación, trasferencia de información, transacciones económicas, acuerdos políticos y sociales, inclusive nuestra información personal cada vez, se vuelve de conocimiento público, pues, cada individuo expone su vida en las diversas plataformas existentes, pues, por el uso inadecuado de la tecnología y la falta de cultura digital, el ser humano brinda las facilidades para convertirse en potenciales víctimas violentando la ley sin mayor esfuerzo.

Es decir, las nuevas tecnologías, se han convertido en un atractivo delincuencial factible para la comisión de diversas modalidades delictivas, pues bien, puede ser objetivo de medio o ataque para la consumación del hecho ilícito, sin mencionar, el anonimato que existe en quien comete la infracción, y la mínima posibilidad de que este llegue a ser descubierto y por consiguiente sancionado, por cuanto esta conductas delictivas suelen quedar en la impunidad. Además, que los perjuicios económicos causados suelen ser superiores a la delincuencia tradicional, ya que, bien se puede señalar, que la información se ha convertido en un valor pecuniario de primera magnitud.

La clasificación de estos delitos, según Acurio (2016), se ha vuelto un reto para el legislativo, pues, la constante innovación tecnológica obliga al manejo de normativa relacionado con la informática, además de un cultura digital en la sociedad a fin de obtener un marco referencial para la prevención y manejo en estas situaciones.

La inexistencia de regulación legal específica y el anonimato son factores criminológicos que favorecen el desarrollo, la expansión y la proliferación de delitos cometidos a través de los medios electrónicos. Ello es así por cuanto no son alcanzados por la ley, creándose situaciones atípicas en las que los principios de legalidad y de tipicidad impiden el juzgamiento y las sanciones correspondientes. A raíz de todo lo expuesto surge la imperiosa necesidad de legislar y así regular el grave problema de los delitos informáticos cada vez más comunes en estos días.

Dentro del ordenamiento jurídico ecuatoriano, los delitos informáticos no abarcan mayor importancia, y esto se evidencia en la escases normativa y regulatoria respecto a los mismos producto de la falta de conexión existente entre la legislación penal y la realidad actual, demostrando la necesidad de regular estas conductas que forman parte de nuestro diario vivir cada vez con mayor normalidad, pues: "los equipos informáticos y las redes telemáticas" deben contar con seguridad suficiente "con el fin de poner obstáculos y luchar contra dichas conductas delictivas, además de la necesidad de tipificar y reformar determinadas conductas, a fin de que estas sean adecuada y positivamente castigadas en el ámbito penal". (Acurio, 2016, p.6).

1. Sujetos del delito informático

Para el estudio de cualquier tipo penal, se requiere la presencia de dos sujetos dentro de la conducta punible, entiéndase como un sujeto activo y otro pasivo, es así como, el titular del bien jurídico lesionado será el sujeto pasivo, y, por otro lado, se considera como sujeto activo de la infracción a quien lesiona el bien jurídico protegido a través de la comisión del tipo penal.

Sujeto Activo

a. Sujeto activo:

El delito como obra humana siempre tiene un autor, aquél que precisamente realiza la acción prohibida u omite la acción esperada. Normalmente en el tipo se alude a dicho sujeto con expresiones impersonales como «el que» o «quien». En estos casos, sujeto activo del delito puede ser cualquiera (delitos comunes), al margen de que después pueda o no ser responsable del delito en cuestión dependiendo de que se dé o no una causa de justificación y de que tenga o no las facultades psíquicas mínimas necesarias para la culpabilidad.

El sujeto activo en un delito informático se caracteriza por su anonimato que le permite evadir su responsabilidad,

Lo expresado es un punto importante, pues en la ejecución de los delitos informáticos, los sujetos activos puede diferenciarse dependiendo su objetivo, si bien es cierto, quienes cometen este tipo de ilícitos lo hacen comúnmente con una finalidad económica, a más de la satisfacción personal de demostrar sus capacidad intelectuales superiores en el uso y manejo de medios electrónicos, no obstante, por otro lado, se encuentran quienes por falta de conocimiento, educación digital o cuidado, sin la intención de delinquir, puedan llegar a cometer el ilícito, por lo que la intencionalidad es un factor fundamental al momento de determinar la pena establecida para estos delitos.

El sujeto activo en los delitos informáticos, como se manifestó en líneas anteriores, posee características que lo diferencian de los delincuentes comunes, pues, para la comisión de la conducta típica, se requiere conocimientos y habilidades en el uso y manejo de sistemas informáticos, particular que genera dificultad en la investigación y persecución por parte de la administración de justicia.

Sujeto Pasivo:

Muñoz Conde (2010) expresa que el titular del bien jurídico es el sujeto pasivo. Empero, no siempre coincide el titular del bien jurídico protegido en el tipo legal con el sujeto sobre el que recae la acción típica. Según Antollicei el sujeto pasivo "es el titular o portador del interés cuya ofensa constituye la esencia del delito" (Antollice, 1960, p.15) pues, como de manera oportuna lo establece Rocco el sujeto pasivo no es necesariamente sobre quien recae la acción.

En este sentido, como bien expresa Rocco (2000), el sujeto pasivo es el titular sobre el cual recae el acto u omisión realizado por el sujeto activo, por ende, al analizar el sujeto pasivo dentro de los delitos informáticos, es importante indicar que no existe mayor diferencia, es decir que la víctima de la comisión de delito, bien puede ser una persona natural, instituciones financieras, entidades gubernamentales, que hagan uso de redes y sistemas informáticos.

Acurio (2016) afirma que la determinación del sujeto pasivo en los delitos informáticos es fundamental para la identificación del ilícito cometido, a pesar de que, a causa del amplio desconocimiento y el modus operandi de los sujetos activos dificulta la aplicabilidad de las acciones pertinentes para prever la consumación del ilícito. Lo expresado es un punto importante, pues, gran parte de los delitos informáticos, no son denunciados ante la autoridad competente, por no ser descubiertos a tiempo, a más de la escasa, por no decir casi nula regulación normativa que brinde protección a las víctimas.

4. El bien Jurídico Protegido en los Delitos Informáticos

La importancia de reconocer el bien jurídico protegido radica en que permite la determinación del injusto del delito, identificar los tipos penales orientando la interpretación de los comportamientos que de estos se derivan, de modo que, se establece como bien jurídico, todo objeto material o inmaterial, derechos, intereses y relaciones, que son valiosos para la sociedad, motivo por el cual, requieren de protección legal. No

obstante, se considera como bien jurídico toda vez que el mismo se encuentre protegido dentro de la normativa vigente del ordenamiento jurídico, y en caso de ser necesario la sanción a dicha conducta otorgue lugar a su vulneración.

Diversos penalistas contemporáneos, salvo pocas excepciones, coinciden en señalar que el Derecho penal protege bienes jurídicos; sin embargo, al definir qué se entiende por bien jurídico es cuando comienzan las diferencias doctrinales.

Los autores Mayer y Lux (2016), determinan que el bien jurídico cumple funciones de gran relevancia para las ciencias penales, pues la afectación a dichos bienes da lugar al castigo punitivo de las conductas que ponen en peligro o lesionan el bien, particular que constituye un requisito fundamental para el ejercicio del ius puniendi.

Resulta obvio señalar la dificultad en la ciencia penal al momento de conceptualizar el jurídico, pues, doctrinariamente, existen tantas definiciones como autores que han desarrollado el tema, dentro de los cuales, es pertinente traer a consideración las siguientes definiciones:

Según Von Liszt (1999), el "bien jurídico" puede ser definido como un interés vital para el desarrollo de los individuos de una sociedad determinada, que adquiere reconocimiento jurídico.

Por otro lado, el padre del garantismo penal Luigi Ferrajoli (2006), manifiesta que la lesión del bien jurídico protegido, debe ser condición necesaria, aunque nunca suficiente para justificar su prohibición y punición como delito.

Así mismo, el profesor Roxin considera que "el bien jurídico, por tanto, es el bien ideal que se incorpora en el concreto objeto de ataque; y es lesionable solo dañando los respectivos objetos individuales de la acción" (Roxin, 1997, p. 63).

Asimismo, Zaffaroni, lo define así: "...bien jurídico penalmente tutelado es la relación de disponibilidad de un individuo con un objeto, protegida por el Estado, que revela su interés mediante la tipificación penal de conductas que le afectan" (Zaffaroni, 1989, p.289).

Ahora bien, para el objeto del presente estudio, se podría decir de forma general que el bien jurídico protegido en los delitos informáticos es la información, misma, que, de acuerdo con el tipo penal, debe ser considera en diversas formas, de modo que, su lesión trasciende a bienes jurídicos secundarios y tradicionalmente protegidos como son: la propiedad, el patrimonio, la seguridad, la intimidad y confidencialidad.

Con base a lo expresado, el bien jurídico dependerá de la conducta del ilícito, es decir, cuando se habla de fraudes informáticos comúnmente el bien jurídico protegido es el patrimonio, en el caso de agresiones a la espera de la intimidad, como el almacenamiento, difusión, publicación, sin autorización a datos personales de terceros, el bien jurídico protegido es la intimidad y la confidencialidad, finalmente si se habla de información o sistemas informáticos el bien jurídico es la propiedad.

Al respecto, acorde a los autores Claudio Magliona y Macarena López (1999) 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". (Claudio Magliona y Macarena López, 1999, p.34).

En definitiva, en la comisión de delitos informáticos, es común que no solo se afecte a un bien jurídico determinando, al contrario, en virtud de la diversidad de conductas, afectan a una diversidad de bienes jurídicos protegidos, poniendo inclusive en conflicto intereses colectivos.

Capítulo 2.- Delimitar el delito informático: apropiación fraudulenta por medios electrónicos dentro del marco jurídico ecuatoriano bajo la modalidad de phishing.

1. El Delito informático y su realidad procesal legal dentro del Ecuador

La primera normativa referente a la regulación de la nuevas tecnologías, tiene lugar con la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas en el año 2002, posteriormente, en el año 2011, el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) emitió la "Estrategia Ecuador Digital" con la cual se inició el desarrollo de Políticas Públicas Sectoriales a fin que las tecnologías de la información y comunicación puedan ser usadas de manera efectiva, en concordación con el desarrollo social, productivo y solidario del Ecuador.

Es así como, en el año 2020 se emitió la Política de Datos Abiertos, de aplicación para las Instituciones de la Administración Pública, a fin de consolidar los procesos de publicación de datos que son generados por estas instituciones.

Uno de los aspectos innovadores fue la incorporación de las infracciones informáticas en el Código Penal, y la expedición del Código Orgánico Integral Penal (en adelante COIP) publicado en el Registro Oficial 180, de 10 de Febrero del año 2014, que conservó varios de los tipos introducidos al Código Penal en el año 2002 e introdujo nuevos tipos penales en lo que respecta a los delitos contra la propiedad que son los que nos interesa analizar en este trabajo.

De acuerdo con la Constitución de la Republica del Ecuador (2008) en su artículo 195 determina que:

> La Fiscalía dirigirá, de oficio o a petición de parte, la investigación pre procesal y procesal penal; durante el proceso ejercerá la acción pública con sujeción a los principios de oportunidad y mínima intervención penal, con especial atención al

interés público y a los derechos de las víctimas. De hallar mérito acusará a los presuntos infractores ante el juez competente, e impulsará la acusación en la sustanciación del juicio penal.

De lo manifestado en líneas anteriores, se desprende que, la investigación pre procesal como procesal se encuentra a cargo de Fiscalía, siendo así, que el resulto de dicha investigación, se convierte en uno de los elementos de convicción que facilitaran el dictamen de la autoridad competente.

Frente a lo expuesto, se desprende la evidente urgencia de elaboración normativa vigente que permita regular y conocer los delitos que se materializan en la red, por ello, es fundamental que nuestro ordenamiento jurídico, cuente con los mecanismos necesarios para prevenir, investigar, y actual de manera efectiva ante el riesgo o cometimiento de delitos informáticos, a fin de proteger los derechos de los ciudadanos y por ende el comedimiento de ilícitos vinculados a la tecnología.

En nuestra legislación, se puede encontrar varias disposiciones legales encaminadas a la protección de datos e información, empero, esta misma diversidad normativa, genera conflicto al no estar acoplada a nuestra realidad actual, pues a pesar de contar con normativa vigente, los ciudadanos se encuentran en una situación de vulnerabilidad, a diferencia de otros países de la región que cuentan con normativa adecuada para la prevención e investigación de estos ilícitos.

Dentro del Código Orgánico Integral Penal (2021), se encuentran tipificados los delitos informáticos cuyos actos se comentan con el uso de las nuevas tecnologías, y lesionen bienes jurídicos protegidos, pues, dichos actos se pueden clasificar en fraude, robo, falsificaciones, suplantación de identidad, espionaje, clonación de tarjetas de crédito, entre otros.

Es importante mencionar que, en el Ecuador, la ciberseguridad se reconoce como uno de los deberes constitucionales del Estado, motivo por el cual, es fundamental, la educación digital a fin de concientizar a la ciudadanía sobre las posibles vulneraciones que puedan llevarse a cabo en el entorno digital, por lo que, es fundamental, fortalecer las capacidades y acciones estatales a fin de garantizar los derechos y libertades, así como la seguridad integral y protección de los bienes jurídicos. (ACUERDO MINISTERIAL 006-2021).

Uno de los problemas que surge al momento de la investigación de delitos informáticos, radica en que nuestro ordenamiento jurídico, no cuenta con convenios internacionales que faciliten los medios idóneos para la determinación del sujeto activo de la información, así como los tratados existentes entre Estados Unidos y Europa. Por tal razón, se manifiesta la complejidad para lograr detectar las cuentas o las direcciones IP que originaron el ilícito, proceso que, dada la naturaleza de los delitos, al consumarse en una esfera virtual y carecer de formalidades, su descubrimiento podría tardar un largo período de tiempo o inclusive nunca llegar a comprobarse.

1.1.Tipos De Delitos Informáticos:

Según Acurio (2016) existen varias formas de cometer un delito informático, las mismas que se han agrupado en cuatro categorías importantes como son: 1) Los fraudes Informáticos; 2) El sabotaje Informático; 3) El espionaje informático; y 4) Los accesos no autorizados a sistemas de información.

1.2.Los fraudes Informáticos:

Dentro de la primera categoría, el fraude informático, se puede considerar como el delito informático más común por su facilidad en comisión, pues para su ejecución no requiere de mayor conocimiento en informática y destreza en la misma, pues consiste en

alterar los sistemas informáticos, además que existe un porcentaje mínimo, o inclusive nulo de descubrir el sujeto activo de la información. (Acurio Del Pino, 2006).

- Los datos falsos o engañosos: manipulación de datos de entrada al ordenador a fin de falsificar movimientos en transacciones pertenecientes a una persona jurídica.
- Manipulación de programas (Caballos de Troya) consiste en modificar y alterar los sistemas informáticos de computadoras.
- Manipulación de los datos de entrada: Se conoce también como sustracción de datos, actualmente es la modalidad de uso común por quien realiza la actividad delictual, pues difícilmente se llega a descubrir la identidad del sujeto activo, mismo que no requiere de mayor conocimientos de informática.
- Manipulación de los datos de salida: Se materializa mediante una vulneración directa al funcionamiento del sistema informático, el ejemplo más claro es la falsificación de instrucción en la fase de adquisición de datos cuando se usa el cajero automático.
- Técnica del salami: En la técnica, mediante repeticiones automáticas, realizar transacciones a penas perceptibles, de una cuenta a otra.
- Phishing: Su objetivo es sustraer la identidad del sujeto pasivo del delito, a través de la obtención de información personal como contraseñas, números de cuenta, de tarjetas de crédito, todo a través del engaño.

1.3.La segunda agrupación es el sabotaje informático,

Se refiere a conductas de alteración, destrucción, deterioro, o actos que impiden el acceso, sobre el objeto material en cuestión, en este caso el sistema informático del ordenador, sin embargo, es importante mencionar, que, dentro de dicha conducta punible,

no abarca solo la desaparición de los datos, por el contrario, la imposibilidad que el titular de estos no pueda disponer ni hacer uso de estos. Samuel Malamud Herrera (2018)

Las modalidades por las cuales se puede cometer sabotajes informáticos son las siguientes:

- Bombas Lógicas: Se basa en un código malicioso, que se inserta y permanece de manera silenciosa en un sistema informáticos, hasta que produce un daño al mismo.
- Gusanos: Se considera como un tipo de virus, pues, su objetivo es infiltrarse en sistemas informáticos, a fin de modificar o eliminar la información contenida en los mismos, por lo que suele generar el colapso de redes informáticas limitando el uso y trabajo de quienes emplean la red.
- Los virus informáticos y malware: Es un tipo de código o clave, que se adhiere a programas informáticos legítimos a fin de modificar el funcionamiento y propagarse de un equipo a otro.
- Es una serie de claves programáticas que pueden adherirse a los programas informáticos legítimos y propagarse a otros.
- Ciberterrorismo o terrorismo informático: Es el uso de herramientas informáticas con la finalidad de atacar y dañar todo tipo de sistema informático que permita causar conmoción social o presión a una entidad gubernamental.

1.4.El tercer grupo es el espionaje informático y el robo o hurto de software.

En esta categoría están los siguientes métodos:

- Fuga de datos (Data Leakage): Conocida también como divulgación de datos reservados no autorizada, pues su objetivo es la sustracción y publicación de la

información confidencial de una empresa.

- Reproducción no autorizada de programas informáticos de protección legal: Dentro de esta modalidad, por lo general causa perjuicio económico a sus víctimas, pues está íntimamente ligado con la piratería informática, pues está vinculado al uso ilegal y al apoderamiento de datos, lista de clientes, balances, etc.

1.5.La cuarta agrupación es el acceso no autorizado a servicios informáticos:

Los principales métodos son:

- Las puertas falsas (Trap doors): Se basa en interrumpir programas informáticos a fin de verificar si los resultados de los procesos complejos son los correctos.
- La llave maestra (SUPERZAPPING): Es un programa informático que permite la apertura de cualquier tipo de archivo, sin importar la protección que este tenga, ya sea para alterarlo, borrarlo, o usar la información que se encuentran contenida en el ordenador.
- Pinchado de Líneas (WIRETAPPING): Se basa en la interferencia de líneas telefónicas que permitan captar la información que se intercepta mediante las mismas.
- Piratas informáticos o Hackers: Esta modalidad, suele efectuarse desde un lugar exterior, vulnerado la seguridad de los sistemas información, además, es común que quienes realicen estos ataques, se identifiquen como usuarios legítimos del sistema, a fin de acceder con mayor facilidad a las contraseñas de acceso que se encuentran dentro del mismo sistema.

2. Delitos informáticos en el Código Orgánico Integral Penal (2021).

Los delitos informáticos ya están tipificados en el marco jurídico legal del Ecuador, tanto en el Código Orgánico Integral Penal (2021), pues en conformidad al artículo 17 del referido cuerpo legal, constituyen los únicos injustos digitales dentro de la ley ecuatoriana, no obstante, se pueden encontrar meros enunciados de delincuencia digital en la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas (2020).

En Ecuador, a partir del 10 de agosto de 2014 con la entrada en vigor del Código Orgánico Integral Penal (2021), se incorporaron conductas relacionadas a delitos informáticos que lesiones bienes jurídicos como: la propiedad, el patrimonio, los datos personales, la intimidad, la seguridad y confidencialidad, mismos que se encuentran articulados en la sección tercera, desde del artículo 178 hasta el artículo 234 del Código Orgánico Integral Penal (2021). Por ende, los delitos informáticos no se encuentran condensados en un capítulo o título específico del referido cuerpo legal, empero, por la naturaleza de las infracciones, son conductas punibles que dogmáticamente encajan en el tipo penal de delito informático.

La siguiente tabla tiene por objeto enunciar de forma clara, el catálogo delitos informáticos que se encuentran contemplados en el ordenamiento jurídico ecuatoriano dentro del Código Orgánico Integral Penal (2021):

Artículo en el COIP	Tipo Penal	Pena	Bien jurídico Protegido

Artículo 168.- Distribución de material pornográfico a niñas, niños y adolescentes. -	La persona que difunda, venda o entregue a niñas, niños o adolescentes, material pornográfico.	pena privativa de libertad de uno a tres años.	la integridad sexual y reproductiva
Artículo 178.- Violación a la intimidad.	- La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio	Pena privativa de libertad de uno a tres años.	la intimidad personal y familiar
Artículo 186.- Estafa. -	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	pena privativa de libertad de cinco a siete años	La propiedad

	tercera, será sancionada con pena privativa de libertad de cinco a siete años. 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.		
Artículo 190.- Apropiación fraudulenta por medios electrónicos. -	La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de	pena privativa de libertad de uno a tres años	La propiedad

	telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años. La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes.		
Artículo 191.- Reprogramación o modificación de información de equipos terminales móviles. -	La persona que reprograme o modifique la información de identificación de los equipos terminales móviles, será sancionada con pena privativa de libertad de uno a tres años.	privativa de libertad de uno a tres años	La propiedad
Artículo 192.- Intercambio, comercialización o compra de información de	La persona que intercambie, comercialice o compre bases de datos que contengan información de identificación de equipos terminales móviles, será sancionada con pena privativa de libertad de uno a tres años.	pena privativa de libertad de uno a tres años.	La propiedad

equipos terminales móviles. -			
Artículo 193.- Reemplazo de identificación de terminales móviles. -	La persona que reemplace las etiquetas de fabricación de los terminales móviles que contienen información de identificación de dichos equipos y coloque en su lugar otras etiquetas con información de identificación falsa o diferente a la original, será sancionada con pena privativa de libertad de uno a tres años	pena privativa de libertad de uno a tres años	La propiedad
Artículo 194.- Comercialización ilícita de terminales móviles. -	La persona que comercialice terminales móviles con violación de las disposiciones y procedimientos previstos en la normativa emitida por la autoridad competente de telecomunicaciones será sancionada con pena privativa de libertad de uno a tres años.	pena privativa de libertad de uno a tres años.	La propiedad
Artículo 195.- Infraestructura ilícita. -	La persona que posea infraestructura, programas, equipos, bases de datos o etiquetas que permitan reprogramar, modificar o alterar la información de	pena privativa de libertad de uno a tres años.	La propiedad

	identificación de un equipo terminal móvil, será sancionada con pena privativa de libertad de uno a tres años. No constituye delito, la apertura de bandas para operación de los equipos terminales móviles.		
Artículo 229.- Revelación ilegal de base de datos. -	La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será	pena privativa de libertad de uno a tres años.	**Seguridad de los activos de los sistemas de información y comunicación**

	sancionada con pena privativa de libertad de tres a cinco años.		
Artículo 230.- Interceptación ilegal de datos. -	Artículo 230.- 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	pena privativa de libertad de tres a cinco años	**Seguridad de los activos de los sistemas de información y comunicación**

	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.		
Artículo 231.- Transferencia electrónica de activo patrimonial. -	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	pena privativa de libertad de tres a cinco años	**Seguridad de los activos de los sistemas de información y comunicación**

	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.		
Artículo 232.- Ataque a la integridad de sistemas informáticos. -	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,	pena privativa de libertad de tres a cinco años.	**Seguridad de los activos de los sistemas de información y comunicación**

	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.		
Artículo 233.- Delitos contra la información pública reservada legalmente. -	La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años. La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años. Cuando se trate de información	pena privativa de libertad de cinco a siete años.	**Seguridad de los activos de los sistemas de información y comunicación**

	reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad.		
Artículo 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones. -	La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios	la pena privativa de la libertad de tres a cinco años.	**Seguridad de los activos de los sistemas de información y comunicación**

	legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.		

3. Apropiación fraudulenta por medios electrónicos

Aspectos como la falta de educación, el avance tecnológico, y la crisis económica, dan lugar a que la delincuencia sea un factor de gran amenaza para el desarrollo para el debido desarrollo socioeconómico de un Estado, pues, la misma, ha evolucionado acoplándose a nuevos métodos, como es el uso de sistemas informáticos y redes electrónicas para delinquir como se evidencia en el presente caso de estudio.

En nuestra legislación, al hablar del delito informático de apropiación fraudulenta por medios electrónicos, es importante destacar que el bien jurídico protegido es la propiedad, no obstante, en otros países de la región, este delito se encuentra en el apartado de delitos económicos, esto en cuanto, a que su comisión, genera tanto un perjuicio individual como colectivo, pues, puede llegar a lesionar a los agentes comerciales, inclusive al orden económico del Estado.

Como indica el Dr. Juan Vizueta Ronquillo (2011), el delito informático en cuestión, era la de apropiación fraudulenta por medios electrónicos la sexta infracción informática incorporada en el Art. 62 de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, que constaba en el capítulo II, "Del robo" y forma parte del Título X "De delitos contra la propiedad" del Código Penal (2012), en su artículo 553 que constaba con el siguiente texto:

> Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren

> fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos. Código Penal (2010)

Del texto expuesto, se desprende como primer subtipo la utilización fraudulenta de medios de información o redes electrónicas, siendo este el verbo rector del delito. El término fraudulentamente tal como consta utilizado se refiere a la intencionalidad que tiene el agente activo del delito. Los medios de los que se debía valer el sujeto activo eran los sistemas de información o redes electrónicas, El objetivo del delito era la apropiación de bienes ajenos.

Como segundo subtipo del articulado, era procurarse la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de esta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos, entendiendo como verbo rector del ilícito procurar, y como verbos complementarios alterar, manipular, modificar.

En ambos casos contemplados en la disposición normativa, la pena privativa de libertad era de seis meses a cinco años.

Actualmente la apropiación fraudulenta por medios electrónicos se encuentra contemplada en el primer inciso del artículo 190 del Código Orgánico Integral Penal (2021):

> La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años.

En el contexto analizado, el delito de apropiación fraudulenta por medios electrónicos determinado en el Código Orgánico Integral Penal, se encuentra redactado de manera muy similar a los términos usados en el Código Penal, a diferencia de ciertos particulares, siendo estos los siguientes:

Dentro de los medios para la comisión de ilícito, se agrega las telecomunicaciones y equipos terminales de telecomunicaciones a las de los ya determinados que son los sistemas informáticos y redes electrónicas, conceptos definidos por la propia Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (2020), en su novena disposición general, define al sistema informático como "todo dispositivo físico o lógico utilizado para crear, generar, enviar, recibir, procesar, comunicar o almacenar de cualquier forma, mensajes datos, mientras y por red electrónica al conjunto de equipos y sistemas de información interconectados electrónicamente"

Además, se suprimió el término mensaje de datos del tipo penal, así como también se modificó la pena, determinado como pena mínima un año y como pena máxima cinco años. De modo que, a más del delito de apropiación fraudulenta por medios electrónicos se ha colocado en un apartado distinto dentro del mismo cuerpo legal, el delito de transferencia electrónica de activo patrimonial, con el objetivo de lograr una mayor protección a los usuarios de las instituciones financieras del país.

3.1.Modalidad de Phishing

Comúnmente el delito de apropiación fraudulenta por medios electrónicos se lleva a cabo mediante una modalidad denominada "phishing", cuyo objeto principal es obtener del usuario (víctima del delito), claves o números de cuentas bancarias para en lo posterior, conseguir un beneficio económico ilícito, de manera fraudulenta mediante el engaño.

El phishing es una modalidad delictiva que ha evolucionado a través del tiempo, es por ellos, que se ha convertido en la modalidad de estafa más usada en la obtención y apropiación ilegitima de datos personales de los usuarios de instituciones financieras, dando lugar al phishing bancario, que tiene como objetivo atacar tanto a los clientes y a los servicios de la banca en línea.

Para Bolaños y Becerra, “consiste en una modalidad de estafa que tiene como objetivo intentar obtener de un usuario sus datos, claves, cuentas bancarias, números de tarjetas de crédito, identidades, etc. En resumen, extrae todas las referencias posibles para después usarlas con fines fraudulentos” (Bolaños, Simone y Becerra, 2005, p.20-21)

Por tanto, la diferencia en la práctica de conductas criminales, se diferencia precisamente en el uso de sistemas informáticos que permiten la ejecución de este tipo de delitos, mismo que se materializan a gran escala y en un corto período de tiempo.

El término phishing proviene de la palabra inglesa "fishing" (pesca), haciendo alusión al intento de hacer que los usuarios "muerdan el anzuelo". Robles (2018)

Al cibercriminal que practica esta técnica se lo conoce como phisher, quien crea una aparente comunicación, comúnmente por correo electrónico, o cualquier medio de comunicación, que le permita suplantar la identidad de una persona, institución o agente

de confianza para el usuario. Pues el objetivo es la entrega de información por parte de la víctima.

El engaño suele llevarse a cabo a través de correo electrónico y, a menudo estos correos contienen enlaces a un sitio web falso con una apariencia casi idéntica a un sitio legítimo. Una vez en el sitio falso, los usuarios incautos son engañados para que ingresen sus datos confidenciales, lo que les proporciona a los delincuentes un amplio margen para realizar estafas y fraudes con la información obtenida.

La principal manera de llevar adelante el engaño es a través del envío de spam (correo no deseado) e invitando al usuario a acceder a la página señuelo. El objetivo del engaño es adquirir información confidencial del usuario como contraseñas, tarjetas de crédito o datos financieros y bancarios. A menudo, estos correos llegan a la bandeja de entrada, disfrazados como procedentes de departamentos de recursos humanos o tecnología o de áreas comerciales relacionadas a transacciones financieras.

Otra forma de propagación, menos común, pueden ser el fax y los mensajes SMS a través del teléfono móvil. En algunos casos se proclamen grandes premios y descuentos en la venta de productos. También se debe destacar que el destinatario de los mensajes es genérico y los mensajes son enviados en forma masiva para alcanzar una alta cantidad de usuarios, sabiendo que un porcentaje (aunque sea mínimo) caerá en la trampa e ingresará al sitio falso, donde se le robará la información.

En efecto, el Phishing o suplantación de identidad consiste en el uso de ingeniería social, a fin de obtener de forma fraudulenta información de carácter persona y confidencial, así como una contraseña, información bancaria y de tarjetas de crédito. para lo cual es pertinente definir a la ingeniería social, como aquel conjunto de técnicas usadas por los ciberdelincuentes, quienes, por medio manipulación o engaño, se aprovechan de

la vulnerabilidad causa por la escasa seguridad de un sistema informática, para que sus víctimas, expongan con facilidad sus datos confidenciales o de su lugar de trabajo.

3.2.Origen y Técnicas del Phishing

Como primer antecedente conocido del término phishing data, tuvo lugar en enero de 1996, pues, surgió la notifica de un grupo de hackers conocidos como alt.2600, aunque es posible que el término ya hubiera aparecido anteriormente en la edición impresa del boletín de noticias hacker 2600 Magazine. Flores (2014)

Ahora bien, como es de conocimiento, no es posible navegar en Internet sin una IP, pues ninguna página web puede mantenerse en la red si no cuenta con una IP anexada, por tanto, es importante para un mejor entendimiento, partir del concepto de una dirección IP, la cual se puede definir como aquella representación numérica única que permite identificar a cualquier dispositivo que se encuentra conectado a internet, mediante el protocolo de redes TCP (Transmission Control Protocol), siendo este el conjunto de normas para la comunicación a través de la web, bien sea por correo electrónico, la transmisión de imágenes o vídeos o la conexión.

Frente a lo expresado, existe una dirección IP privada como publica, se entiende como IP publica aquella a la cual se puede acceder de manera directa desde internet, es decir, dicha dirección es visible en toda la web, pues al ingresar a la misma desde cualquier dispositivo electrónicos conectado a la red, se obtiene una dirección IP publica que es suministrada por el proveedor de la conexión a internet, de modo que su uso es ligeramente más seguro, pero con mayor visibilidad. Por otro lado, una dirección IP privada, es aquella que su propio router de red asigna su dispositivo, es decir, permite que

los dispositivos que se encuentran conectados a la misma red, se comuniquen entre sí para poder conectarse entre sí.

No obstante, el conflicto surge cuando se produce la suplantación de IP, mediante la codificación de IP que conllevan una dirección de origen con cierta modificación que permite ocultar la identidad del emisor o suplantar el sistema informático en cuestión, particular que puede desarrollarse mediante diversas técnicas que a modo de ejemplo serán desarrollas a continuación.

En su mayoría, dentro de las técnicas de Phishing más usuales es la modificación en el diseño del correo electrónico, a fin de suplantar el enlace que en apariencia sería el correcto, un ejemplo de lo manifestado, es el uso de direcciones que contenga el carácter arroba, es decir, el enlace http:/www.google.com@members.tripod.com/ puede engañar a un observador casual y hacerlo creer que el enlace va a abrir en la página de www.google.com, cuando en realidad el enlace redirecciona al usuario a otra página web.

En el mismos sentido, otros de los métodos popular de Phishing, se sirve en supuestos ataques a la víctima, bajo el mismos código del portal web que está suplantando, por tanto, dirige al usuario a iniciar sesión en la propia página del banco o servicio, donde la URL y los certificados de seguridad parecen correctos, posterior a ello los usuarios reciben un mensaje solicitando la verificación de la cuenta, para lo cual se adjunta un enlace, mismo que esta modificado y permite proceder con el ataque.

Otro problema que se presenta respecto a las URL, se menciona en cuanto al nombre de dominio internacionalizado de los navegadores, ya que, a simple vista, la similitud que conduce a otros sitios, suele ser casi exacta, es así, que, al usar esta técnica, se pretende dirigir a los usuarios a otros portales web a fin de realizar una conducta contraria a la intención inicial del usuario**.**

Capítulo 3.- Falencias del delito informático: apropiación fraudulenta por medios electrónicos en el Ecuador.

1. Situación Internacional

Es evidente la necesidad de un consenso internacional en las valoraciones político-jurídicas de los problemas que surgen por el uso indebido de medios y dispositivos electrónicos, situación que ha dado lugar a la modificación de los derechos penales nacionales. Acurio (2016)

Para un mejor entendimiento de la situación internacional respecto a los delitos informáticos, es importante indicar que en 1983 la Organización de Cooperación y Desarrollo Económico (OCDE) inició un estudio de la posibilidad de aplicar y armonizar en el plano internacional las leyes penales, a fin de luchar contra el problema del uso indebido de los programas de computación. Es pertinente indicar que, respecto a la delincuencia informática, esta puede generar implicaciones de carácter económicos que bien pueden ser de índole internacional como transnacional, y el riesgo de en cuanto a la diversa protección jurídico-penal nacional, bien puede generar un perjuicio ante el flujo legítimo de información.

Años más tarde, en 1986 la OCDE emitió un informe titulado Delitos de informática: análisis de la normativa jurídica, en el cual se mencionaba la normativa vigente y las propuestas de reforma para ciertos Estados miembros, recomendando, mediante una lista, las conductas que los estados podrían sancionar y prohibir en su normativa penal, tales como: el fraude y la falsificación informática, la alteración de datos y programas de

computadora, sabotaje informático, acceso no autorizado, interceptación no autorizada y la reproducción no autorizada de un programa de computadora protegido.

A fin de concluir con el informe indicado en líneas precedentes, el Consejo de Europa tuvo la iniciativa de desarrollar un estudio que permite crear directrices que faciliten al legislativo al momento de determinar la conducta punible, considerando los derechos y libertades de los ciudadanos y la protección de estos.

En el mismo sentido, el Comité, Especial de Expertos sobre Delitos relacionados con el empleo de las computadoras, del Comité Europeo para los problemas de la Delincuencia, tomó a consideraciones particulares como la protección de la víctima, la prevención e investigación de la delincuencia informática, a través de la cooperación internacional.

El Consejo de Europa aprobó la recomendación R (89)9 sobre delitos informáticos, misma que fue adoptada por el Comité de Ministros del Consejo de Europa el 13 de septiembre de 1989, dentro de la cual se recomendó a los Estados miembros, mantener una legislación vigente a la realidad actual, haciendo hincapié en la delincuencia vinculada al uso de computadoras.

En 1990 la Organización de las Naciones Unidas (ONU) en el Octavo Congreso sobre Prevención del Delito y Justicia Penal, celebrado en La Habana, Cuba, determinó que la ciberdelincuencia era fruto del aumento en el uso de datos en la economía y burocracia de los estados. Años más tarde, la OCDE, elaboró varias normas encaminadas a la protección de los sistemas de informáticos, con el objetivo de crear bases tanto para los gobiernos como para el sector privado. Pues como señala el Dr. Acurio (2016) en su libro Delitos Informáticos, si bien estos organismos han pretendido el desarrollo normativo en materia de delitos informáticos, la responsabilidad de que dichas normas sean acopladas dentro del ordenamiento jurídico es de cada Estado.

A pesar de que actualmente, los Estados cuenten con normativa vigente que regule los delitos informáticos, existe una problemática evidente a escala internacional por la limitada cooperación que existen, pues la falta de consenso sobre la definición de conducta delictiva, los escases en la investigación a más de la dificultad procesal que presente, impidiendo el cumplimiento de la normativa y cumplimiento de la ley.

Torres y otros (2015), expresan que, en el contexto internacional, pocos son los países que cuentan con normativa apropiada y las medidas pertinentes para enfrentar la problemática que abarca los delitos informáticos, entre ellos, se puede destacar: Estados Unidos, Alemania, Austria, Gran Bretaña, Holanda, Francia, España, Argentina y Chile.

1.1.Convenio Sobre Cibercriminalidad de Budapest.

El Convenio sobre Cibercriminalidad, Convención sobre Delitos Informáticos, Convenio sobre Ciberdelincuencia o Convenio de Budapest, es el único acuerdo internacional que abarca cubre todas las áreas relevantes de la legislación sobre ciberdelincuencia (derecho penal, derecho procesal y cooperación internacional) y propone una política penal contra la ciberdelincuencia.

Campos (2019), expresa que en el año 2001 el Consejo de Europa elaboró el Convenio de Budapest sobre la ciberdelincuencia, el proyecto destinado a armonizar las legislaciones de sus 47 Estados miembros y 8 observadores a la fecha. Fue adoptado por el Comité de Ministros del Consejo de Europa en su sesión N°. 109 del 8 de noviembre de 2001, se presentó a firma en Budapest, Hungría, el 23 de noviembre de 2001 y entró en vigor el 1 de julio de 2004.

Actualmente países como Argentina, que ha basado su ley de delitos informáticos en este Convenio, Australia, Ecuador y Sudáfrica, están evaluando su adhesión.

Como señala Morón Lerma (2002), el Convenio de Cibercriminalidad persigue básicamente tres objetivos en torno a los cuales se estructura, a saber: armonizar el Derecho Penal material, establecer medidas procesales o cautelares adaptadas al medio digital y poner en funcionamiento un régimen rápido y eficaz de cooperación internacional.

El objetivo del convenio es garantizar la seguridad informática, a través de una política penal común que permita proteger a la sociedad frente a la ciberdelincuencia, mediante una debida implementación legislativa a la par de la cooperación internacional.

En el presente convenio, se establecen directrices normativas de cooperación internacional enfocadas a la creación de procesos penales encaminados a combatir los delitos informáticos, no obstante, Gómez (2010) expresa que, a pesar del contenido tanto jurídico como legal que conlleva el presente convenio, el Ecuador de momento, no se encuentra suscrito a este acuerdo, particular que limita la lucha efectiva contra los delitos informáticos, no obstante, su proceso de adhesión se encuentra en trámite.

El convenio consta de cuatro capítulos, el Capítulo I abarca tanto definiciones como un amplio glosario para mejor comprensión, por otro lado, Campos (2019) expresa que el Capítulo II, determina los penales referentes a la confidencialidad, la integridad, disponibilidad de los datos y sistemas informáticos. En el Capítulo III se enuncian los principios que deben aplicarse en beneficio de la cooperación internacional, a la extradición, a la asistencia mutua, así como los procedimientos en ausencia de acuerdos internacionales aplicables. Finalmente, el último Capítulo IV menciona la firma y la entrada en vigor, adhesión al Convenio, es decir todo lo relativo a disposiciones finales.

2. Principios que regulan la aplicación de los Delitos Informáticos.

2.1.Problemática Territorial.

La red se ha convertido en uno de los medios factibles para infringir la ley, pues, una de sus características principal es que no atiende a un espacio territorial determinado, situación que dificulta la determinación del sujeto activo de la infracción del delito informático, de igual manera, lo considera Flores (2014), al expresar que de entre los rasgos característicos de las nuevas redes informáticas, lo que interesa para la investigación es la supra territorialidad.

En el mundo físico, el delito se materializa en un lugar determinado o determinable dentro del territorio nacional, permitiendo que el mismo se someta a la jurisdicción y competencia nacional en materia penal, empero, los delitos cometidos en el espacio digital, han dejado de lado los principios de localización de conductas delictivas tradicionales, al no ser cometido en un espacio físico.

Desde el punto de vista diversos doctrinarios como Flores (2014), han manifestado la posibilidad de una rama del Derecho supranacional, misma que mencionaría disposiciones legales uniformes, que abarquen no solo la penalización de conductas referentes a delitos informáticos, sino, toda relación jurídica que incluya medios electrónicos, como el comercio electrónico, los contratos por internet, las transferencias financieras, entre otras.

Pues, de lo manifestado en líneas anteriores, García (2015) afirma la necesidad de que toda normativa vigente dentro del ordenamiento jurídico, debe ajustarse a la realidad informática, de forma preventiva, ms no de manera reactiva, una vez que el daño se encuentre consumado, pues, la idea es garantizar la titula efectiva de los derechos, bienes y libertades de los ciudadanos en beneficio del interés colectivo.

Por su parte, Giménez (2006) determina que la problemática territorial no es la única dificultad en la investigación de los delitos informáticos, pues, en materia probatoria, la dificultad de identificar al sujeto activo del ilícito por encontrarse fuera del alcance de la competencia de la autoridad competente, quedando estos casos en impunidad, o inclusive, el caso de ser identificado no es posible que responda penalmente al encontrarse fuera del territorio, como lo es comúnmente.

Por lo expresado, difícilmente se podría considerar el ejercicio de la Función Judicial fuera del territorio nacional, es decir, que, a la víctima de un delito informático, no se le puede garantizar la tutela judicial efectiva de sus derechos. (Muñoz, 2000).

En este sentido, Hernández (2009) se demuestra la necesidad de que el Derecho Penal, en virtud del incontrolable avance tecnológicos, que han dado lugar a nuevas conductas delictivas, opere de forma conjunta con el denominado Derecho Informático.

2.2.Principio de extraterritorialidad

Acurio (2016). Expresa que el principio de extraterritorialidad se encuentra constituido por los siguientes principios: principio de la nacionalidad o personalidad, el principio de la defensa y el principio de la universalidad y justicia mundial.

2.3.El principio de la nacionalidad o personalidad:

El artículo 15 de la Declaración Universal de los Derechos Humanos establece que ‘’la nacionalidad puede definirse como el vínculo jurídico y político que liga a una persona con un Estado determinado por el que se obliga con él mediante relaciones de lealtad y fidelidad y se hace acreedor a su protección diplomática’’.

> Es el principio que justifica la aplicación de la ley penal a hechos cometidos fuera del territorio del Estado en función de la nacionalidad del autor (principio de la

> nacionalidad activo) o del titular del bien jurídico lesionado o puesto en peligro por el delito (principio de la nacionalidad pasivo. (Bacigalupo, 2007, p.182)

Por lo expresado, se entiende que al momento de imputar la sanción a quien cometió el delito, solo se le puede imponer la ley que corresponde a su nacionalidad, es decir la normativa de su país de origen, independientemente del lugar en el cual se haya cometido el ilícito, partiendo de la naturaleza misma del principio que es la obediencia legislativa del ciudadano al Estado, a pesar de no encontrarse dentro del mismo, cuestión que actualmente no se aplica de forma frecuente. El artículo 15 del Código Orgánico Integral Penal (2021) guarda armonía con lo descrito en líneas precedentes, debido a que la disposición mencionada determina que toda normativa contenida en el cuerpo legal penal se aplica a todo sujeto de nacionalidad ecuatoriana o extranjera que ejecute una conducta punible.

2.4.El principio de la defensa

Para la aplicación de este principio, se considera la afectación a la integridad territorial, por ende, la nacionalidad del bien jurídico protegido, es decir, el lugar en el cual se materializo el delito, mas no la nacionalidad del sujeto activo, por lo que queda en juego la protección de bienes naciones. Acurio (2016).

Ha sido tomado por algunos países, como por ejemplo en el caso Ecuador, se puede realizar un trámite para solicitar la extradición de un criminal informático que haya vulnerado bienes jurídicos protegidos en la nación como resultado de la realización de la infracción penal. Claro que esta norma no puede ser aplicada en todos los países ya que algunos de ellos como el nuestro prohíben la extradición de ecuatorianos que hayan cometido una infracción en otro país, en este caso se aplica un principio de equivalencia, es decir si el delito cometido en el otro país se encuentra tipificado en el nuestro también puede seguirse el proceso penal por el cometimiento de dicho delito,

pero en nuestro país.

2.5.El principio de la universalidad y justicia mundial

El Diccionario de la Real Academia Española (2001) define al principio de justicia mundial como:

> Principio en virtud del cual los tribunales de un determinado país ejercen su jurisdicción sobre crímenes internacionales de especial gravedad, sobre la base de la naturaleza del delito, sin tomar en consideración ni el lugar donde fue cometido, ni la nacionalidad de su autor.

El Principio de Justicia Universal, de Jurisdicción Universal o de Justicia Mundial permite la aplicación de justicia en el orden internacional, es así como, puede conocer, investigar, juzgar y ejecutar lo juzgado respecto a un crimen en los siguientes casos:

Se trate de bienes jurídicos necesarios de protección en el ámbito internacional, y el lugar en el cual se realizó el ilícito, o en su país de origen no sean procesados, no se asuma el caso, o no puedan ser juzgados, ya sea porque el Estado se inhiba de conocer, o no cuente los medios legales adecuados investigar, juzgar y condenar, es así como cualquier país del mundo puede hacer justicia, esto en conformidad de los postulados de la buena fe, determinados en los denominados Principios de Princeton: "El Estado ejercerá la jurisdicción universal de buena fe y de conformidad con sus derechos y obligaciones de derecho internacional" (Torres, 2013, p.12)

3. Principio de extraterritorialidad frente al delito de apropiación fraudulenta por medios electrónicos.

3.1.Código Orgánico Integral Penal

3.1.1. Apropiación fraudulenta por medios electrónicos

La legislación ecuatoriana, ha determinado que la apropiación fraudulenta por medios electrónicos, constituye una conducta penal relevante dentro del Derecho Penal del Ecuador, es así como, a continuación, se procederá a analizar la tipicidad objetiva y subjetiva de la mentada infracción, la cual se encuentra contenida en el artículo 190 del Código Orgánico Integral Penal (2021), la cual establece:

> La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años.

La tipicidad objetiva del injusto citado, se configura de la siguiente manera:

Con respecto al sujeto activo de la infracción, se establece que es de naturaleza genérica, es decir, cualquier persona. Si bien, es común que, para la comisión de delito de apropiación fraudulenta por medios electrónicos, el sujeto activo de la infracción, tenga conocimientos técnicos y avanzados en tecnología, no es menos cierto, que un individuo sin conocimientos informáticos, puede contactar a un profesional de los sistemas digitales, para que ejecute la labor material de la infracción, existiendo una especie de autoría mediata en la ejecución del hecho punible. Por tanto, bajo lo expuesto, a criterio personal, es correcto que el sujeto activo de la infracción estudiada, sea de naturaleza genérica.

Por su parte, el sujeto pasivo, también ostenta naturaleza genérica, es decir puede ser cualquier persona. El sujeto pasivo de este delito, tiene un carácter amplio, pues el

perjudicado de la infracción podría ser una persona natural, instituciones financieras, personas jurídicas que hagan uso de sistemas informáticos o plataformas de comercio digitales.

Con respecto al verbo rector, al igual que en el Código Penal extinto, es ´´utilizar'' fraudulenta de medios de información o redes electrónicas para facilitarse un bien ajeno, por cuanto, el núcleo duro del tipo penal, es utilizar fraudulentamente, entendiéndose al verbo utilizar como "emplear, usar, manejar, servirse, beneficiarse, disfrutar, gastar, consumir, aprovechar, dedicar, destinar, aplicar".

Por otro lado, otro verbo rector existente, es el de procurar la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, de modo que, el verbo rector ''procurar'', hace alusión a intentar, pretender, esforzarse, emprender, empezar, tratar, proyectar, trabajar, proporcionar, etc.

Otros verbos rectores presentes en el delito en cuestión son alterar, manipular y modificar el funcionamiento de programas o redes informáticas.

Con respecto al bien jurídico protegido, se afirma que es el patrimonio y propiedad una persona, ya que, al tratarse de un delito informático de apropiación ilícita, el bien jurídico protegido es sin duda el derecho a la propiedad, empero, a su vez, se afirma que también pueden llegar a lesionarse otros bienes jurídicos como la intimidad personal y la seguridad nacional, etc. Pues dicha situación dependerá de cómo se realice la conducta típica.

El objeto material de la infracción consiste en bienes, derechos o valores de naturaleza digital, contenidos dentro de los sistemas informáticos.

Finalmente, con respecto a los elementos necesarios para que se configure la presencia de la infracción, se analiza el elemento del fraude, entendido el mismo como el engaño realizado por el autor de la infracción, a fin de vulnerar sistemas informáticos que sirvan como medio para la ejecución del hecho punible.

Tipicidad Subjetiva:

Finalmente, con respecto a la tipicidad subjetiva, se afirma que es de naturaleza dolosa, es decir, como expresa Welzel (1970), es necesario que el individuo ostente conciencia y voluntad de los elementos que caracterizan a la conducta de apropiación fraudulenta por medios electrónicos como penalmente relevante.

3.1.2. Principio de extraterritorialidad

La potestad punitiva (el *ius puniendi*) de los Estados forma parte inescindible del ejercicio de su soberanía y en tal medida, se encuentra sometida a límites determinados por el espacio sobre el que tal soberanía se ejerce. En principio, por tanto, la potestad punitiva estatal no puede ejercerse más allá de las fronteras del propio Estado.

Frente a la impunidad existente a causa de la ejecución de delitos informáticos, el derecho penal, se ha visto en la necesidad de brindar justicia de forma extraterritorial, pues de esta forma, se pretende evitar la lesión a bienes jurídicos protegidos. Torres (2013)

Es así como, Cárdenas (2008), menciona que, al hablar del delito de apropiación fraudulenta por medios electrónicos, se refiere a delitos de distancia, pues, por lo general, la conducta se inicia en un lugar distinto a su consumación, por lo que es pertinente la elaboración de normativa que permita determinar la jurisdicción penal al caso.

Ahora bien, dentro del ordenamiento jurídico ecuatoriano, si el delito de apropiación fraudulenta por medios electrónicos, es cometido fuera del territorio

nacional, el sujeto activo del ilícito estará sujeto a las disposiciones legales, si dentro del territorio nacional se ha producido efectos del hecho punible y el responsable no ha sido juzgado por la evidente evasión ante su juzgamiento.

Con respecto a la legislación ecuatoriana, el Código Orgánico Integral (2021), en su artículo 14, determina las reglas de aplicación del principio de extraterritorialidad penal, las cuales se expone a continuación, a fin de concluir con la explicación doctrinaria y legal del mismo:

> Las normas de este Código se aplicarán a:
>
> 1. Toda infracción cometida dentro del territorio nacional.
>
> 2. Las infracciones cometidas fuera del territorio ecuatoriano, en los siguientes casos:
>
> a) Cuando la infracción produzca efectos en el Ecuador o en los lugares sometidos a su jurisdicción.
>
> b) Cuando la infracción penal es cometida en el extranjero, contra una o varias personas ecuatorianas y no ha sido juzgada en el país donde se la cometió.
>
> c) Cuando la infracción penal es cometida por las o los servidores públicos mientras desempeñan sus funciones o gestiones oficiales.
>
> Cuando la infracción penal afecta bienes jurídicos protegidos por el Derecho Internacional, a través de instrumentos internacionales ratificados por el Ecuador, siempre que no se haya iniciado su juzgamiento en otra jurisdicción.
>
> e) Cuando las infracciones constituyen graves violaciones a los derechos humanos, de acuerdo con las reglas procesales establecidas en este Código.

3. Las infracciones cometidas a bordo de naves o aeronaves militares o mercantes de bandera o matrícula ecuatoriana.

4. Las infracciones cometidas por las o los servidores de las Fuerzas Armadas en el extranjero, sobre la base del principio de reciprocidad.

3.2. Imposibilidad práctica de la aplicación del principio de extraterritorialidad frente al delito de apropiación fraudulenta por medios electrónicos.

La ejecución del delito informático de apropiación fraudulenta promedios electrónicos es de carácter, pues como se desarrolló con anterioridad, el delincuente puede estar en un país mientras que la víctima en otro, situación, que general una total dificultad, pues, el principio de territorialidad impide que se puedan hacer investigaciones acerca de un delito con características de transnacionalidad.

El uso excesivo de las nuevas tecnólogas, ha dado lugar al denominado ciberespacio, mismos que ha generado nuevas formas delictivas que desbordan la territorialidad de los ordenamientos jurídicos (Díaz, 2010).

> A pesar del legislador, prever la posibilidad de delitos que sean cometidos fuera del territorio nacional, sin embargo, para su aplicación debe cumplir con una de las condiciones establecidas en el inciso segundo del art 14 del Código Orgánico Integral Penal, sin embargo, pocos son los casos en los que se ha aplicado este criterio, pues, a beneficio práctico del juzgador se pretende ajustar al lugar donde se cometieron los hechos, es así, por lo que la característica de transnacional de la delincuencia informática es otro de los problemas de perseguibilidad. Tradicionalmente se ha considerado que la ley penal solo se aplica en el territorio de la República, hecho que constituye el llamado “principio de territorialidad de la ley (Acurio, 2010, p. 56).

En el mismo sentido, Flores (2014) considera que la nueva dimensión que supone la aparición del ciberespacio ha desbordado claramente los principios de localización delictiva tradicionales, basados en el principio de territorialidad. En el mundo físico, el delito se produce en un lugar más o menos determinado del territorio, o al menos cabe partir del territorio para asigna la jurisdicción nacional y la competencia interna en materia penal.

De lo manifestado se desprende, la dificultad permanente de juzgar y sancionar el delito de apropiación fraudulenta por medios electrónicos, en caso de sus efectos materializarse fuera del territorio nacional, por cuanto, la extraterritorialidad se ha convertido en un problema jurídico que da lugar a un vacío legal, pues, al este delito presentarse en un escenario transnacional, no estaría sujeto a regulación o jurisdicción alguna. Sin mencionar la complejidad en la determinación del sujeto activo de la infracción, ya que, difícilmente se encuentra bajo la competencia del ente investigar.

Finalmente, es importante indicar, que a pesar del Estado contar con las sanciones penales para el delito informático de apropiación fraudulenta por medios electrónicos, se presume que actualmente, la misma solo podría aplicarse en caso que el delito sea cometido dentro del territorio nacional, más no, cuando este sea realizado por personas que se encuentre en otros Estados, donde las condiciones de validez, responsabilidad penal y normativa, sea totalmente distintas, limitando la atribuibilidad de la responsabilidad al sujeto activo del delito en mención. (Aboso, Zapata, 2006).

3.3.Impunidad en la administración de justicia sobre los delitos informáticos

Le Clercq, Cháidez y Rodríguez (2016), puede entenderse la impunidad como la evasión o el escape de la sanción que implica una falta o un delito. Lo habitual es que la impunidad se produzca cuando, por motivos políticos o de otro tipo, una persona que es responsable de haber violado la ley no recibe el castigo correspondiente y, por lo tanto,

sus víctimas no reciben ninguna reparación. En este sentido, la impunidad no es más que libertad para quien comete el ilícito, al lograr quedar absuelto de responsabilidad.

Como señala Jesús Rodríguez:

> La impunidad es un acicate para la comisión de nuevos delitos. Las acciones delincuenciales que quedan sin castigo efectivo y adecuado estimulan y, con frecuencia, escalan nuevas prácticas de criminalidad. (Rodríguez, 2011, p.7)

En cuanto a los delitos informáticos en relación con la administración de justicia se ha podido evidenciar el incremento de la impunidad, por la falta de normativa, y medios adecuados para la investigación y juzgamiento de estos delitos, pues, se debe entender desde la función legislativa, que no es posible aplicar los mismos preceptos legales para aquellas conductas que bien pueden materializarse en espacios físicos en el territorio.

El delito informático, como se ha venido desarrollando en el presente trabajo de investigación, es una nueva modalidad delictiva a consecuencia del mal uso de las nuevas tecnologías, por lo que, es lógico, la existencia de vacíos jurídicos que brinden una adecuada protección a los bienes jurídicos que puedan verse afectados ante estas nuevas conductas criminales.

En base a esta normativa se entiende que un acto se vuelve punible cuando cumple ciertos elementos probatorios o también conocidos como elementos de convicción. Los elementos de convicción son el conjunto de pruebas electrónicas necesarias para probar un delito, sin las cuales se entiende la imposibilidad de colocar una pena a este ilícito.

Dentro de nuestro marco jurídico penal ecuatoriano, la dirección de la investigación recae sobre el fiscal, de forma conjunta con la policía judicial y al grupo de investigadores civiles de la Dirección Nacional de Investigaciones de la Fiscalía General del Estado, no obstante, a pesar de que el Código Orgánico Integral Penal, incorporan tanto normativa

como mecanismos que en teoría permitirían contrarrestar estas conductas, en la práctica, la falta de medios investigativos idóneos impide que se pueda consolidar elementos necesarios que permitan determinar la responsabilidad del titular del hecho punible.(Acurio, 2015).

Un acto es considerado como punible una vez que cumpla con los elementos de convicción necesarios, es así como, en el caso de los delitos informáticos, es necesario probar la existencia y materialidad del delito, pues, a más de ser una de las etapas procesales más útil dentro de la investigación, pues sin esta, sería imposible la determinación del delito. Acurio (2019)

Para el delito objeto del presente estudio, resulta dificultoso determinar los elementos de convicción, pues al ser cometidos mediante medios electrónicos, es importante indicar que no hay límite en cuanto a fronteras dentro de los sistemas informáticos, por lo que, resulta casi imposible determinar al operador del delito.

En definitiva, la impunidad en la investigación en los delitos informáticos ha generado que los mismos se encuentren en ascenso, ocasionando la falta de credibilidad al proceso de instrucción fiscal, por lo que, es obligación del estado garantizar la protección y prevención de estas conductas.

Conclusiones y Recomendaciones

Entonces, el delito informático como todo acto o conducta penalmente relevante que ostente la finalidad de causar lesión o puesta en peligro a un bien jurídico protegido mediante el uso de instrumentos electrónicos, digitales e informáticos. Por cuanto, en concordancia a la doctrina, se puede definir al delito informático como la acción que reúne las características propiamente del delito, es decir que sea un acto típico, antijuridico, culpable, atribuible a su autor, empero, para su debida consideración, se requiere la implementación de un elemento informático o telemático al momento de su comisión, con el objetivo de causar daño a bienes jurídicos protegidos, derechos y garantías reconocidos dentro del ordenamiento jurídico y que, son susceptibles de ser sancionadas por el Derecho Penal.

Ahora bien, para el objeto del presente estudio, se podría decir de forma general que el bien jurídico protegido en los delitos informáticos es la información, misma, que, de acuerdo con el tipo penal, debe ser considera en diversas formas, de modo que, su lesión trasciende a bienes jurídicos secundarios y tradicionalmente protegidos como son: la propiedad, el patrimonio, la seguridad, la intimidad y confidencialidad.

Aspectos como la falta de educación, el avance tecnológico, y la crisis económica, dan lugar a que la delincuencia sea un factor de gran amenaza para el desarrollo para el debido desarrollo socioeconómico de un Estado, pues, la misma, ha evolucionado acoplándose a nuevos métodos, como es el uso de sistemas informáticos y redes electrónicas para delinquir como se evidencia en el presente caso de estudio.

En nuestra legislación, al hablar del delito informático de apropiación fraudulenta por medios electrónicos, es importante destacar que el bien jurídico protegido es la propiedad, no obstante, en otros países de la región, este delito se encuentra en el apartado de delitos económicos, esto en cuanto, a que su comisión, genera tanto un perjuicio

individual como colectivo, pues, puede llegar a lesionar a los agentes comerciales, inclusive al orden económico del Estado.

Por su parte, la potestad punitiva (el *ius puniendi*) de los Estados forma parte inescindible del ejercicio de su soberanía y en tal medida, se encuentra sometida a límites determinados por el espacio sobre el que tal soberanía se ejerce. En principio, por tanto, la potestad punitiva estatal no puede ejercerse más allá de las fronteras del propio Estado.

Frente a la impunidad existente a causa de la ejecución de delitos informáticos, el derecho penal, se ha visto en la necesidad de brindar justicia de forma extraterritorial, pues de esta forma, se pretende evitar la lesión a bienes jurídicos protegidos

La legislación ecuatoriana, ha determinado que la apropiación fraudulenta por medios electrónicos, constituye una conducta penal relevante dentro del Derecho Penal del Ecuador, la cual se encuentra tipificada en el artículo 190 del Código Orgánico Integral Penal (2021).

La ejecución del delito informático de apropiación fraudulenta promedios electrónicos es de carácter, pues como se desarrolló con anterioridad, el delincuente puede estar en un país mientras que la víctima en otro, situación, que general una total dificultad, pues, el principio de territorialidad impide que se puedan hacer investigaciones acerca de un delito con características de transnacionalidad.

El uso excesivo de las nuevas tecnólogas, ha dado lugar al denominado ciberespacio, mismos que ha generado nuevas formas delictivas que desbordan la territorialidad de los ordenamientos jurídicos.

Por consiguiente, es importante indicar, que a pesar del Estado contar con las sanciones penales para el delito informático de apropiación fraudulenta por medios electrónicos, se presume que actualmente, la misma solo podría aplicarse en caso que el

delito sea cometido dentro del territorio nacional, más no, cuando este sea realizado por personas que se encuentre en otros Estados, donde las condiciones de validez, responsabilidad penal y normativa, sea totalmente distintas, limitando la atribuibilidad de la responsabilidad al sujeto activo del delito en mención.

Entonces, se recomienda lo siguiente:

- Es importante que la normativa penal en materia de delitos informáticos sea actualizada de forma constante en virtud del acelerado avance tecnológico, personalmente se cree, que es necesaria la elaboración de un reglamento que desarrolle el alcance jurídico de los delitos informáticos establecidos en el Código Orgánico Integral Penal (2021), debido a que, de la investigación del presente trabajo se desprende que dichos injustos adolecen de ambigüedad, incertidumbre e ineficacia material.
- El Estado, a fin de precautelar los derechos de los ciudadanos, debe promover e informar sobre las medidas de prevención en materia de delitos informáticos.
- A fin de mejorar las técnicas de investigación para la determinación del responsable del delito informático, es necesaria la creación de una Unidad Especializada de la Policía Nacional, que cuente con especialistas en temas informáticos que ostenten la capacidad para perseguir infracciones digitales y entreguen a la Fiscalía General del Estado, las herramientas necesarias para la investigación y ejercicio de la acción penal correspondiente, permitiendo que se pueda encontrar elementos de convicción, y posteriormente en el proceso, medios probatorios que presenten la posibilidad de responsabilizar a quienes ejecutan el hecho punible informático.
- A los usuarios de servicios en línea de instituciones financieras, tomar en consideración, que, en caso de un supuesto contacto por parte de la institución, que

solicite información de carácter sensible, para mayor certeza y verificación, tener contacto con una fuente confiable que acredite pertenecer a la institución financiera con el objetivo de evitar ser víctima de un delito informático.

REFERENCIAS BIBLIOGRÁFICAS

1. Aboso, G; Zapata, M. (2006). Cibercriminalidad y Derecho Penal. Madrid: Editorial B d F.
2. Acurio Del Pino, S. (2016). *Delitos informáticos: generalidades*. EDIAR.
3. Acurio del Pino, S. (2019). Manual de manejo de evidencias digitales y entornos informáticos. Versión 2.0.
4. Acurio, S. (2015). Derecho Penal Informático. Quito: Corporación de Estudios y Publicaciones.
5. Antollicei, F. (1960). *Manual de Derecho Penal*. UTHEA.
6. Aravena, C. C. El lugar de comisión de los denominados ciberdelitos.
7. Bacigalupo, E, (2007) *Derecho Penal. Parte General*. Ed. Hammurabi.
8. Bolaños, Simone y Becerra, J. (2005). Phishing Nueva Forma de Ciberestafa. Revista "Giga N° 3, 20,21. Coruña. E. Lapt.
9. Campos, N. J. O. (2019). *Normativa Legal sobre Delitos Informáticos en Ecuador*. *Revista Científica Hallazgos21*, *4*(1), 100-111.
10. Chinchón, J. (2014). *Impunidad, sistema de justicia, estado de Derecho y democracia. ¿Es peor la inmunidad que el crimen en sí mismo*? Revista del Centro de Investigación y Estudios Judiciales.
11. Díaz, A. (2010). El delito informático, su problemática y la cooperación internacional como paradigma de su solución: el convenio de Budapest, Revista electrónica del Departamento de Derecho de la Universidad de la Rioja.

12. Española, R. A., & Madrid, E. (2001). *Diccionario de la lengua española* (Vol. 22). Madrid: Real academia Española.

13. Ferrajoli, L. (2006). *Garantismo penal* (Vol. 34). UNAM.

14. Flores, L. (2014). *Derecho informático*. Editorial Larousse – Grupo editorial patria.

15. García, I. (2007). La reforma penal de la falsificación, tráfico y uso ilícito de tarjetas bancarias, IDP: revista de Internet, derecho y política.

16. Giménez, J. (2006). Delito e informática: algunos aspectos de derecho penal material, Eguzkilore: cuaderno del Instituto Vasco de Criminología, 20, 197 – 215.

17. Gómez, A. D. (2010). El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest. *Revista Electrónica de Derecho de la Universidad de La Rioja (REDUR)*, (8), 169-203.

18. Hernández, L. (2009). *El delito informático*. Eguzkilore: Cuaderno del Instituto Vasco de Criminología, 23, 227-243.

19. Huerta, M., & Líbano, C. (1996). *Delitos informáticos*. Ed. Jurídica ConoSur.

20. Le Clercq, J; Cháidez, A y Rodríguez, G (2016), Midiendo la impunidad en América Latina: Retos conceptuales y metodológicos. Revista de Ciencias Sociales.

21. Magliona Markovicth y López Medel, C. (1999). *Delincuencia y Fraude Informático*. Editorial Jurídica.

22. Markovicth, C. P. M., & Medel, M. L. (1999). *Delincuencia y fraude informático: derecho comparado y ley n 19.223*. Editorial Jurídica de Chile.

23. Mayer Lux, L. (2017). *El bien jurídico protegido en los delitos informáticos*. Revista chilena de derecho, 44(1), 261-285.

24. Miranda, M. H., & Manzur, C. L. (1996). *Delitos informáticos*. Editorial Jurídica

Conosur.

25. Muñoz Conde, F. (2010). *Derecho Penal General*. Tirant Lo Blanch.
26. Ramírez Bejerano y Aguilera Rodríguez: *Los delitos informáticos. Tratamiento internacional*. Contribuciones a las Ciencias Sociales.
27. Robles Sotomayor, F. M., & Mory Arciniega, E. C. (2018). Derecho Procesal Penal I: manual autoformativo interactivo.
28. Rocco, A. (2000). *El objeto del delito y de la tutela jurídica penal. En Dogmática y Criminología*. Legis.
29. Rodríguez, J. R. (2011). La impunidad y la fractura de lo público. *Impunidad: síntoma de un Estado ausente*, *6*.
30. Torres, H. (2013). *La extraterritorialidad de la ley penal: el principio de justicia universal, su aplicación en Colombia Prolegómenos*. Derechos y Valores, *16*(31), 99-115.
31. Torres, H. (2013). La extraterritorialidad de la ley penal: el principio de la justicia universal, su aplicación universal en Colombia. Revista Prolegómenos. Derechos y Valores
32. Torres, J.; Soto, J; Landaverde, M. (2000). *Delitos informáticos*. Universidad de El Salvador.
33. Vizueta Ronquillo, J. U. (2011). Delitos informáticos en el Ecuador. Guayaquil, Ecuador: Editorial Edino
34. Von Liszt, F.n (1999). *Tratado de Derecho penal*. Reus.
35. Welzel, H. (1970). *Derecho Penal Alemán*. Editorial Jurídica de Chile.
36. Zaffaroni, E. (1989). *Manual de Derecho Penal*. Ediar.

Normas Jurídicas

1. Código Orgánico Integral Penal, Registro Oficial Nro. 180. (Asamblea Nacional 10 de agosto de 2021).
2. Constitución de la República del Ecuador, Registro Oficial 449. (Asamblea Nacional 20 de Octubre de 2008).
3. Código Penal, Registro Oficial 147. (Asamblea Nacional 15 de febrero 2012).
4. Convenio Sobre Cibercriminalidad de Budapest, Convenio 185. (Consejo de Europa 8 de noviembre de 2001).
5. Ley de Comercio Electrónico Firmas, y Mensajes de Datos, Registro Oficial 557. (Asamblea Nacional 08 de diciembre de 2020).