



Universidad Tecnológica ECOTEC

Facultad de Derecho y Gobernabilidad

Título del trabajo:

Análisis del proceso de identificación del sujeto activo en el delito de Apropiación Fraudulenta por Medios Electrónicos en el Ecuador en el año 2021.

Línea de Investigación:

Gestión de las Relaciones Jurídicas

Modalidad de titulación:

Proyecto de Investigación

Carrera:

Derecho con énfasis en ciencias penales y criminológicas

Título a obtener:

Abogado de los Tribunales de la República del Ecuador

Autor (a):

José André Yari Bustamante

Tutor (a):

Mgtr. María Soledad Murillo Ortiz

Guayaquil – Ecuador

2023

Contenido

Introducción	1
Antecedentes	2
Planteamiento del problema	4
Pregunta problema	4
Objetivo general	4
Objetivos específicos	4
Justificación	5
Marco Teórico	7
Delitos electrónicos	7
Historia	7
Concepto de delitos informáticos	8
Características de los Delitos Informáticos	9
Caracteres del Delito Informático	10
Delito de apropiación fraudulenta por medios electrónicos en Ecuador	12
La Omisión impropia	13
Modalidades más conocidas en el ámbito de la apropiación fraudulenta por medios electrónicos o fraude informático	15
Proceso de identificación del sujeto activo del delito	17
Proceso penal ecuatoriano	17
Criminalística	18
Indicios y evidencias en el entorno digital	22
La prueba	23
Problemas para la persecución del sujeto activo en los delitos informáticos	25
Territorialidad de los delitos informáticos.	25
Medios en los que se almacena la información digital	27

Anonimidad en internet	28
Incidencia del delito de apropiación fraudulenta por medios informáticos en Latinoamérica	29
Ecuador	29
Colombia	30
Perú	31
España	32
Mecanismos de cooperación internacional	33
Convenio de Budapest	33
La Convención de la Organización de las Naciones Unidas para el combate de la Delincuencia Organizada Transnacional	38
Elac 2018	38
Interpol	39
Tratados de cooperación jurídica internacional	40
Metodología de la Investigación	43
Enfoque de la Investigación	43
Método de la investigación	43
Descriptiva	43
Explicativa	44
Período y Lugar de la Investigación	44
Universo y Muestra de la Investigación	44
Procesamiento y análisis de la información	45
Análisis e interpretación de los resultados.	47
Análisis del proceso penal No. 01613201700483	47
Análisis del proceso por contravención No. 0928620146178	50
Análisis estadístico de la incidencia del delito de apropiación fraudulenta por medios electrónicos y similares	54

Conclusiones	56
Recomendaciones	58
Bibliografía	59

Índice de tablas

Tabla No. 1.....	54
------------------	----



ANEXO N°16

**CERTIFICADO DE APROBACIÓN DEL TUTOR PARA LA PRESENTACIÓN DEL
TRABAJO DE TITULACIÓN CON INCORPORACIÓN DE LAS OBSERVACIONES
DE LOS MIEMBROS DEL TRIBUNAL**

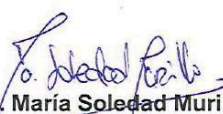
Samborondón, 08 de diciembre de 2023

Magíster
Andrés Madero
Decano(a) de la Facultad
Derecho y Gobernabilidad
Universidad Tecnológica ECOTEC

De mis consideraciones:

Por medio de la presente comunico a usted que el trabajo de titulación TITULADO: **Análisis del proceso de identificación del sujeto activo en el delito de Apropiación Fraudulenta por Medios Electrónicos en el Ecuador en el año 2021**, según su modalidad PROYECTO DE INVESTIGACIÓN; fue revisado y se deja constancia que el estudiante acogió e incorporó todas las observaciones realizadas por los miembros del tribunal de sustentación por lo que se autoriza a: **José André Yari Bustamante** para que proceda a la presentación del trabajo de titulación para la revisión de los miembros del tribunal de sustentación y posterior sustentación.

ATENTAMENTE,

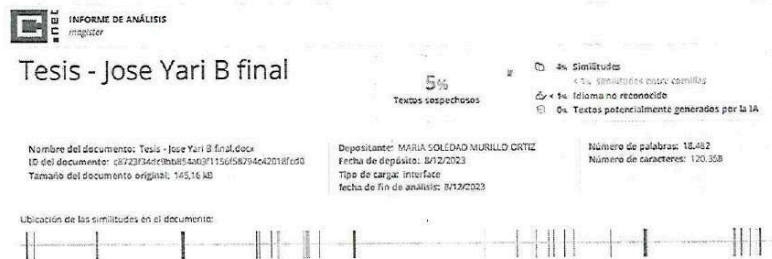

Mgtr. María Soledad Murillo Ortiz

Tutora

CERTIFICADO DEL PORCENTAJE DE COINCIDENCIAS

Habiendo sido nombrado Mgtr. María Soledad Murillo Ortiz, tutor del trabajo de titulación “Análisis del proceso de identificación del sujeto activo en el delito de Apropiación Fraudulenta por Medios Electrónicos en el Ecuador en el año 2021.” elaborado por José André Yari Bustamante, con mi respectiva supervisión como requerimiento parcial para la obtención del título de Abogado.

Se informa que el mismo ha resultado tener un porcentaje de coincidencias del 5% mismo que se puede verificar en el siguiente link: [file:///D:/Descargas/detailed-report_es_tesis-jose-yari-b-final%20\(2\).pdf](file:///D:/Descargas/detailed-report_es_tesis-jose-yari-b-final%20(2).pdf). Adicional se adjunta print de pantalla de dicho resultado.




FIRMA DEL TUTOR
Mgtr. María Soledad Murillo Ortiz

Dedicatoria

A mi madre, con amor.

Resumen

El presente trabajo de investigación aborda el proceso de identificación del sujeto activo en el delito de apropiación fraudulenta por medios electrónicos desde; en primer lugar, el marco doctrinario desde su origen y desarrollo, hasta cuales son las características que posee y las formas más comunes en las que se manifiesta. Así también se establecen las reglas procesales específicas que se emplean en este delito y en los delitos electrónicos en general en términos probatorios y periciales. Se realiza también una síntesis de la incidencia de esta conducta en diversos países cercanos de la región y otros conocidos por tener una normativa mucho más desarrollada en este tema. Por último analizaremos las herramientas mancomunadas con las que cuentan los estados para el combate de este tipo de crímenes.

Palabras clave: delitos electrónicos, apropiación, fraude, medios electrónicos, Convenio de Budapest.

Abstract

This research work addresses the process of identifying the active subject in the crime of fraudulent appropriation by electronic means from; Firstly, the doctrinal framework from its origin and development, to what characteristics it has and the most common forms in which it manifests itself. This also establishes the specific procedural rules used in this crime and in electronic crimes in general in evidentiary and expert terms. A summary is also made of the incidence of this behavior in various nearby countries in the region and others known to have much more developed regulations on this issue. Finally, we will analyze the joint tools that states have to combat this type of crime.

Keywords: Cybercrime, appropriation, fraud, electronic media, Budapest Convention.

Introducción

El ser humano, por su naturaleza, busca constantemente mediante las ciencias e investigación nuevas tecnologías que a lo largo de la historia han representado cambios en las dinámicas de la sociedad a todos los niveles, este constante desarrollo y evolución pone a ciencias como el Derecho cada cierto tiempo frente a escenarios por regular en pro de que sostener el orden social y los derechos humanos.

Uno de los elementos que su desarrollo nos ha cambiado la vida, es la red de comunicación e información, el internet. El internet; en 2022, fue usado según datos del Instituto Nacional de Estadísticas y Censos por el 78,5% de la población ecuatoriana, con la incidencia reciente de la pandemia, el porcentaje de usuarios creció de un 66,7% en 2019. (INEC, 2022)

Con el notablemente elevado porcentaje de uso de estas nuevas herramientas de comunicación, y los correspondientes medios por las cuales se emplean, es lógico establecer que el mundo en general ha atravesado un cambio paradigmático, siendo el internet una vía muy eficaz para comunicar que actualmente cuenta con muchísimas formas de emplearlo, desde mensajes instantáneos a través de aplicaciones, hasta video conferencias que pueden reunir a cientos de personas.

Cuando hablamos de comunicación y uso de internet, tenemos que considerar que además de las conexiones interpersonales, el internet se ha convertido en la forma de conectar empresas con usuarios, instituciones financieras con usuarios, sistemas estatales que pueden ir desde los sistemas tributarios hasta los de tránsito con el usuario, es así que además de servirnos como herramienta de comunicación e información el internet y en general los medios informáticos, han reemplazado un sin número de actividades que se realizaban en el pasado de manera presencial o manual. Considerando esta situación; y como pasa en la mayoría de situaciones en las que se involucran miembros de la sociedad, estos escenarios adquieren o reflejan características de las mismas, tanto desde el punto de vista positivo como negativo, así se crea una nueva problemática en las actividades desarrolladas a través de

medios informáticos que el derecho en los últimos años ha buscado hacerle frente, que son el auge de los delitos cometidos a través de estos medios y los delitos que tienen como objetivo a los medios informáticos propiamente dichos.

Como reflejo de la sociedad, el uso de medios electrónicos en nuestro día a día, se presenta como un escenario para el auge de conductas delictivas, así tenemos el nacimiento de dos grandes grupos de delitos, que aunque contengan elementos similares, son muy distintos. En un grupo tenemos los que atacan directamente a los medios informáticos, para alterar su disponibilidad, integridad u obtener la información que los mismos contengan. En el segundo grupo tenemos los que emplean los medios informáticos como puente, y que son en la práctica la evolución de delitos tradicionales; tal como nuestro objeto de estudio, el delito de apropiación fraudulenta mediante medios informáticos, para muchos doctrinarios y ordenamientos jurídicos, está contenido dentro del delito de estafa. (Pino S. A., 2015)

Estos dos grupos de delitos, comparten varias características similares, y que para la delincuencia, son muy llamativas, puesto que resultan en acciones cuyo balance riesgo recompensa es muy positivo e implican bajo riesgo de ser procesados; es a este escenario que los estamentos jurídicos alrededor del mundo buscan hacerle frente, creando herramientas tanto para los encargados de las etapas previas de investigación como para los juzgadores, para llegar sancionar efectivamente los mismos y de alguna manera precautelar el orden en el mundo informático.

Antecedentes

El interés del derecho por este tipo de delitos tiene un desarrollo más bien corto, actualmente ya se encuentran insertados en la mayoría de los ordenamientos jurídicos en vigencia alrededor del mundo. Aunque el origen de histórico de la denominación de delitos informáticos provenga de la literatura fantástica de los años 80, ya en los 60 se presentaron los primeros casos de ataques a medios informáticos, sobre todos los orientados hacia las comunicaciones telefónicas, generando grandes pérdidas a empresas líderes de ese mercado y que involucraron caras que hoy en día son muy conocidas

en el mundo tecnológico como Jobs y Wozniak, fundadores de Apple. (Feced, 2023)

De esta manera el crimen informático fue evolucionando y adaptándose a las nuevas formas de la tecnología, que también iba constantemente creando barreras para la prevención de conductas anti jurídicas. Sin embargo, la acción regulatoria del derecho, no se concreta hasta finales de los 90, cuando un grupo de países se reunió para estudiar los problemas que se originaban del uso del internet. (Zambrano Mendieta, Dueñas Zambrano, & Macías Ordoñez, 2016)

En el Ecuador, el primer intento de regular este tipo de conductas, se dio en la ley publicada en 1999 relativa al comercio electrónico, cuyo enfoque incluía primordialmente la protección de los intercambios comerciales que se daban en medios electrónicos así como la privacidad de los usuarios sin embargo incluyo todo un capítulo a lo que en su momento denominó Infracciones Informáticas. (Machuca, 2012)

El delito informático en sentido amplio, ha despertado el interés de la ciencia jurídica, estudiar los elementos que los componen y elaborar distintos mecanismos para lograr una sanción oportuna de los mismos, como la unificación de criterios a niveles regionales, la firma de tratados que versan sobre la delincuencia informática, etc. Diversos estudios han determinado ya las problemáticas principales que enfrentan el combate a estos crímenes, como que puedan estar dirigidos hacia cientos o miles de personas, que el riesgo es muy bajo, puesto que no es necesario un vínculo físico cercano con la víctima, siendo que incluso pueden cometerse desde otros países; considerando estas situaciones, y así la investigación en torno a estas conductas continua puesto que la evolución de los mecanismos para su materialización está en constante desarrollo.

Planteamiento del problema

Tomando en cuenta lo planteado, consideramos de especial importancia evaluar el estado en el que actualmente se encuentra nuestro sistema jurídico para el combate y prevención de la apropiación a través de medios electrónicos, siendo que esta conducta es; en términos estadísticos, la que mayor presencia tiene, según información de la Fiscalía General del Estado (2021) durante 2021 se registra un total de 3.962 denuncias sobre este delito, muchas de las cuales no llegarán a la determinación de un responsable.

Para hacer una evaluación más efectiva, se realizará una consideración de la incidencia del delito objeto de esta investigación, en diversos países en Latinoamérica la manera en cómo se ha tipificado en sus ordenamientos jurídicos y los mecanismos de cooperación existentes en la región. Por último, se abordarán los mecanismos empleados a nivel global para el combate de este delito, en donde encontraremos distintos convenios que buscan unificar criterios normativos y de punibilidad de este tipo de delitos.

Pregunta problema

¿Cuáles son las debilidades del ordenamiento jurídico ecuatoriano para la identificación del sujeto activo en el delito de apropiación fraudulenta por medios electrónicos, en comparación con la normativa vigente en España?

Objetivo general

Analizar el proceso de identificación del sujeto activo en el delito de apropiación fraudulenta por medios electrónicos en el Ecuador en el año 2021.

Objetivos específicos

- Determinar, haciendo uso de la doctrina disponible, el delito de apropiación fraudulenta por medios electrónicos.
- Analizar la incidencia de este delito a nivel regional en el período 2021.
- Comparar los mecanismos normativos a nivel regional vigentes en Latinoamérica.

Justificación

En la actualidad, considerando el contexto explicado previamente, según el Sistema Integrado de Actuaciones Fiscales (SIAF) de la Fiscalía General del Estado la cantidad de delitos electrónicos denunciados ha aumentado exponencialmente, esto evidentemente guarda relación con el cambio de las dinámicas sociales que produjo la pandemia del COVID 19, en el tema que centraremos nuestro trabajo de investigación señala que entre 2020 y 2021 la incidencia de la apropiación fraudulenta por medios electrónicos aumento en 1682 casos denunciados, es decir alcanzo un pico mayor del 73,7% respecto al período anterior. (Ciberdelitos, 2021)

Situación parecida nos encontramos con el resto de los denominados delitos electrónicos que se encuentran sancionados por nuestro Código Orgánico Integral Penal, cuyo índice ha ido en aumento acelerado; este aumento en la incidencia de este tipo de delitos evidentemente tiene un impacto en la sociedad, evidentemente mellando la confianza de los usuarios en los medios electrónicos, sobre todo los empleados para el comercio.

Por lo que se pone de manifiesto la importancia y necesidad del estudio de este delito, tanto para entender el porqué de su necesidad y las cuestiones doctrinarios que rodean a estos nuevos tipos de delitos; pero también para identificar las debilidades de nuestro sistema actual para su fortalecimiento, tanto desde el punto de vista procesal, hasta identificar con que herramientas normativas de mancomunidad a nivel regional cuenta el país para el combare de los efectos transnacionales de este tipo de delitos.

Por último, sirva el presente trabajo para que la ciudadanía en general comprenda las formas en las que puede manifestarse el delito estudiado, para condicionar nuestras conductas y dirigirlas hacia la minimización de los riesgos potenciales, pero también para conocer que tipo de conductas que podemos encontrar en los entornos digitales son sancionables o no.

MARCO TEÓRICO

CAPÍTULO I

Marco Teórico

Delitos informáticos

Historia

Al día de hoy escuchar los términos delito informático, ciber delincuencia o criminalidad informática, se ha convertido en algo común y necesario en el día a día de una sociedad que funciona prácticamente en todos sus ámbitos apoyada de alguna manera por la tecnología, la información o el internet.

A pesar del contexto actual del delito electrónico, en donde podemos encontrar formas de materializar muy complejas los mismos, han llegado hasta ese punto siguiendo un largo camino de evolución, encontrando sus primeros rastros en los años sesenta en donde la literatura fantástica hacía mención en sus obras más populares de la posibilidad de utilizar las computadoras con un fin distinto al que fueron concebidas, en pro de causar daño. (Sain, 2015)

Culminando los años sesenta en los Estados Unidos el movimiento hippie en conjunto con los programadores se manifestaron en contra del contexto bélico que dividía al país debido a la guerra de Vietnam, haciendo uso de un mecanismo mediante el cual podían hacer uso gratuito del sistema telefónico; a los que se les denominó phreaks, que eran personas expertas en redes telefónicas que mediante la identificación de los tonos que utilizaban los operadores podían conocer cómo se direccionaban las llamadas, de este movimiento surgieron importantes en la tecnología como el Steve Wozniak y Steve Jobs. (Gallo, 2010)

Sin embargo, no es hasta la década de los ochenta que se declara a una persona culpable de un delito cibernético. Ian Murphy fue encontrado culpable de hacking o acceso no consentido a un medio informático de un tercero sin consentimiento con el fin de copiar o manipular la información, siendo que este accedió a los sistemas de una compañía telefónica estadounidense manipulando su reloj interno consiguiendo que los usuarios puedan hacer llamadas gratis en horas pico. (Pascual, 2015)

Con el surgimiento y desarrollo del internet nacieron las primeras formas de sabotaje informático, es así que tenemos como en 1988 Robert Morris creó lo que se conocería como el primer gusano de internet, que pasó de ser un ejercicio inocente a convertirse en una forma masiva de boicotear sistemas informáticos llegando a afectar a la Fuerza Aérea de los Estados Unidos y diversas universidades . (González, Meana, & López, 2015)

Y así las formas de manipulación informática han ido evolucionando, hasta convertirse en sistemas complejos que requieren una profesionalización especial para su uso, pero también han encontrado su espacio para aportar positivamente al desarrollo tecnológico puesto que hoy en día es muy común que las grandes compañías dedicadas a la seguridad informática recluten a reconocidos hackers para poner a prueba sus sistemas.

Concepto de delitos informáticos

Los delitos en general implican conductas antijurídicas tipificadas en la norma, en la ley, que por lo general describen conductas comúnmente conocidas como el robo, estafa, defraudación, etc. Este tipo de delitos previo a la evolución tecnológica, que el mundo ha sufrido eran abordados por la teoría penal desde un único punto de vista, sin embargo las necesidades del mundo actual, han obligado a la normativa penal a evolucionar hacia el mundo virtual, así se da origen a los delitos electrónicos.

Las primeras menciones de esta nueva esfera de delitos, tuvieron su origen en Francia durante la fundación del G8, que entre sus objetivos planteados tenía analizar la creciente criminalidad en el entorno específico del mundo del internet, que se encontraba en pleno apogeo y crecimiento, utilizando ese término para abarcar todo tipo de conducta delictiva que se llevaba acabado en esta red. (Manjarres & Jimenez, 2012)

Según la profesora García Cantizano (2012) los delitos informáticos son aquellos en los que para su cometimiento se emplea un sistema automatizado para procesar datos o transmitirlos. Esta definición tiene un carácter amplio y general, sin embargo este tipo de delitos han sido conceptualizados o

analizados desde la perspectiva de cómo se utiliza la tecnología para conseguir el fin de la conducta delictiva. Sobre este particular otros tratadistas los consideran como las conductas típicas, antijurídicas, culpables y punibles en los sistemas informáticos desempeñan un papel; sea este para la materialización de un delito actuando como medio para un fin o el objeto del delito sea el propio sistema informático en sí.

Como podemos observar no existe un concepto único sobre los delitos informáticos, en general la doctrina ha ido adoptando conceptos amplios que con el tiempo se han ido moldeando, de la misma forma los legisladores han ido confeccionando las normas para sancionar este tipo de conductas, sin profundizar en el aspecto conceptual para definir los mismos, manteniendo incluso y, a pesar de los esfuerzos de distintas Convenciones conformadas por diversos países, muchas diferencias muy notorias incluso a nivel regional.

Características de los Delitos Informáticos

Partiendo del hecho de que los delitos informáticos guardan una estrecha relación con el sistema de procesamiento de datos, se reflejan en ellos las mismas características de estos, y de todo el comportamiento que pueda llevarse a cabo en el mundo virtual, tales como que las mismas pueden ser consideradas como conductas de tipo criminógenas enmarcadas en los delitos denominados de cuello blanco; en este sentido también tenemos que considerar que se realizan en situación de privilegio debido a un estatus o posición dentro de una organización aprovechando una ocasión creada dentro de dichas funciones, por lo que se pueden considerar también organizacionales; por esto mismo, pueden producir severos daños o pérdidas de carácter económico, puesto que además es muy fácil conseguir un gran rédito de este tipo de delitos. Siendo que también los mismos ofrecen facilidades para conseguir la impunidad, puesto que se pueden realizar en segundos, y desde prácticamente cualquier sitio, es decir no permiten el establecimiento sencillo de un nexo físico entre el delincuente y el objeto del delito; esto, acompañado de lo sofisticados que pueden llegar a ser además del conocimiento técnico necesario para su análisis provocan que sean pocas las

denuncias que se presenten al respecto y que sean muy pocos los casos que lleguen a conseguir una sanción de derecho, por su facilidad pueden ser cometidos por personas con un amplio rango de edad y pueden tener como objetivo áreas militares o comprometidas. (Salgado, Robalino, & Pazmiño, 2021)

Caracteres del Delito Informático

Como los demás delitos especificados en la normativa penal, los delitos informáticos tienen caracteres que los definen.

Sujetos de los delitos informáticos.

Las conductas penalmente sancionadas implican para la configuración de las mismas, la existencia de al menos dos sujetos, el sujeto que comete el delito o sujeto activo y el sujeto que recibe o es víctima de la conducta o sujeto pasivo; y, que la conducta tenga por objeto un bien jurídico que se encuentre específicamente por la ley. Estas son las características básicas de un delito penal, a continuación realizaremos un análisis más detallado de cada uno de los caracteres específicamente enfocado en los delitos informáticos.

Sujeto Activo

En resumidas cuentas el sujeto activo de un delito penal es quien realiza la conducta descrita por el tipo penal, en el específico caso de los delitos informáticos; como se mencionaba anteriormente, este sujeto posee características especiales tales como la formación y el conocimiento para el manejo de los sistemas informáticos, y una posición que le permita llevar a cabo los mismos.

A pesar de ser una forma delictiva nueva los tratadistas han encontrado coincidencias entre las formas de describir a los sujetos activos de este delito, enmarcándolos en teorías criminológicas clásicas como las de los delitos de cuello blanco. El acercamiento a esta teoría se da no solamente por el bajo impacto social que pueda tener este tipo de delitos cuando el bien jurídico protegido que llevan por objeto es un bien económico, sino que, su

correspondencia con esta teoría se da porque no existe en los sujetos activos típicos de los delitos informáticos una necesidad de delinquir, por ende no puede explicarse esta conducta por el estado de pobreza, e incluso al necesitar de una formación específica, no se puede explicar desde el punto de vista de la falta de educación. (Pino S. A., 2015) Llegando a ser descritos por Tiedemann (1985) como un hecho penal profesional.

Sujeto pasivo

El sujeto pasivo en los delitos penales es el titular del bien jurídico protegido descrito por el tipo penal. En los delitos informáticos como se mencionaba anteriormente, existe una facilidad que otros tipos de delitos no poseen para atacar a distintos sujetos yendo, desde una persona natural hasta toda una estructura gubernamental, sin la necesidad de mayor infraestructura para la materialización del mismo. El acceso amplio a distintas potenciales víctimas es un efecto colateral del desarrollo voraz del acceso a la tecnología alrededor del mundo.

Bien Jurídico Protegido

El bien jurídico protegido es uno de los aspectos más relevantes para la identificación de un delito, los mismo pueden abarcar objetos materiales, intangibles o derechos, cuya importancia en la sociedad o lo relevantes que pueden ser para el desarrollo de la misma, requieren de un resguardo especial a través de la ley.

El bien jurídico protegido es definido por Von Liszt (Leal, 2021) como aquel que tiene para la sociedad y el desarrollo de sus individuos un interés vital. En el caso de los delitos informáticos en términos generales los tratadistas coinciden en que el bien jurídico protegido es la información; pero considerando a esta como la llave de entrada para afectar otros bienes jurídicos. Por ejemplo, en el caso de la apropiación fraudulenta empleando medios electrónicos, se necesita en un primer término atacar el bien jurídico protegido de la información, puesto que esta es la llave de resguardo para acceder a la materialización del delito que busca afectar al bien jurídico tutelado por la

norma como es el patrimonio. Así podemos concluir que otro de los rasgos característicos y específicos de este tipo de delitos es que en el camino hacia la adecuación de su conducta con el tipo penal establecido en la norma penal vigente afectan no solo a un bien jurídico protegido sino a varios, como pueden ser el patrimonio, la información, la intimidad, la propiedad, etc. (Lux, 2017)

Delito de apropiación fraudulenta por medios electrónicos en Ecuador

En el Ecuador en el Código Orgánico Integral Penal vigente se describen varios tipos de delitos informáticos, a pesar de que los mismos no se encuentran reunidos en un mismo capítulo puesto que como se mencionaba anteriormente pueden afectar a más de un bien jurídico protegido, entre los delitos enlistados en la normativa encontramos el delito objeto de este estudio, que menciona que 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”. (Fiscalía General del Estado, 2020)

Este delito está contemplado en nuestra normativa como un tipo penal destinado a proteger el tipo penal denominado propiedad, a diferencia de como se lo considera en otros países en donde se lo cataloga netamente dentro de los delitos económicos. El mismo está incluido en nuestra normativa desde los primeros lineamientos establecidos en las infracciones informáticas descritas en la ley relativa al comercio electrónico publicada en 1992 en su artículo 62. (Machuca, 2012)

Del análisis de lo mencionado en el COIP vigente y los caracteres mencionados anteriormente que componen los tipos penales, podemos decir que el delito de apropiación fraudulenta interviene:

- Sujeto activo, según lo descrito en el artículo 190 del COIP el sujeto activo de este delito es de tipo no calificado, puesto que la redacción del mismo no especifica la necesidad de poseer una característica en particular. Sin embargo, por su naturaleza y aunque la normativa no lo especifique, este delito necesita o requiere de tener conocimientos calificados en el ámbito informático, para procurar el uso fraudulento de un sistema, este establecimiento del sujeto activo tan poco preciso recae en el hecho de que para el legislador este tipo de delito se acerca mucho a la estafa, que puede ser llevada a cabo por cualquier sujeto sin que medie una característica especial o particular, sin embargo no cualquier sujeto puede manejar una sistema informático de la forma y para los fines descritos en el tipo penal.
- Sujeto pasivo, en este delito el sujeto pasivo que sufre la afectación patrimonial, los mismos que pueden ser desde un único individuo, hasta un grupo de individuos, persona jurídica, institución financiera o gubernamental.
- Conducta Punible, el legislador en la redacción del tipo penal, establece en primer término la utilización fraudulenta de un sistema informático de manera general, en lo subsiguiente menciona más específicamente la adecuación conductual a la que se refiere, considerando la alteración, mala utilización o negligente puesta en funcionamiento de redes electrónicas, programas, sistemas telemáticos y equipos de telecomunicaciones, encajando todas estas conductas en el marco de lo que se considera utilizar fraudulentamente un medio electrónico. En este sentido y dadas las características de este tipo de delitos, es necesario recalcar que la manipulación a la que se hace referencia no implica ningún contacto material directo con el medio electrónico empleado.
- Perjuicio, al igual que en el delito de estafa, la adecuación al tipo penal que implica una pena, exige que exista la materialización del perjuicio; en este caso patrimonial, del sujeto pasivo. Mismo que debe ser cuantificable, evidente y comprobable, sobre el cual no quepan dudas.

La Omisión impropia

Además de los elementos característicos que configuran un delito como los señalados previamente, la apropiación fraudulenta por medios electrónicos, doctrinariamente se ha vinculado con otras figuras jurídicas. Es el caso de la omisión impropia, la misma se define como la falta de acción de parte de quién funge como garante para evitar la materialización de una conducta lasciva, lo que le atribuye responsabilidad de tipo penal. (Cifuentes, 2021)

Pero por qué es relevante esta figura en el delito investigado, como se ha venido analizando a lo largo del presente trabajo, el delito de apropiación fraudulenta tiene un medio, o un canal por el que se materializa y encaja en la conducta sancionada penalmente, esto es un medio de tipo electrónico, que bien podría ser una computadora, un smartphone, una aplicación o una página web. En el caso del perjuicio material que busca el criminal al perpetrar estos delitos, previo a conseguirlo, hay una vulneración a un medio electrónico y sus seguridades, en muchos casos dichos medios electrónicos que fungían como guardianes del patrimonio afectado los usamos previa aceptación de un contrato o acuerdo, como es el caso por ejemplo de las aplicaciones bancarias.

Cabe analizar, en el presente trabajo, si la contraparte que representa jurídicamente al medio electrónico vulnerado es susceptible de responsabilidad penal y en qué casos. Para ejemplificar esta figura jurídica nos centraremos en los casos en los que el servicio vulnerado sea uno de tipo bancario o monetario. Al respecto nuestra carta magna manifiesta en su artículo 54 manifiesta que las cualquier persona o entidad que oferte un servicio de tipo público dirigido u orientado a producir y comercializar bienes considerados de consumo, serán susceptibles de responsabilidad de tipo civil o penal, en caso de prestar un servicio deficiente, defectuoso o que no se de conforme a lo publicitado. (Asamblea Constituyente, 2008, pág. 27)

Considerando esto, en efecto, en el caso de la apropiación fraudulenta por medios electrónicos, es perfectamente aplicable la figura de la omisión impropia al reunir los elementos de tener el mandato constitucional de brindar un servicio de calidad, que abarca tomar los resguardos correspondientes para

prevenir riesgos, por ende se convertiría en responsable por omisión en caso de que el análisis del juzgador lo considere. Esto acorde además por lo señalado en el Código Monetario, que señala que las instituciones financieras son susceptibles de asumir responsabilidad penal.

Modalidades más conocidas en el ámbito de la apropiación fraudulenta por medios electrónicos

Como mencionamos anteriormente las formas de manipular un sistema informático, pueden ir desde mecanismos muy sencillos hasta formas muy complejas entre las más conocidas actualmente, tenemos el denominado phishing que es una técnica como su nombre lo indica en la que los criminales buscan pescar o inducir al error a la víctima mediante el uso de un cebo de apariencia legítima. Esto lo consiguen a través de correos electrónicos que pueden ser enviados a millones de usuarios con una programación tal que al activarlo el usuario le da acceso al criminal a un lugar previamente identificado como clave para materializar la apropiación del patrimonio de la víctima.

Otra de las más reconocidas formas de phishing; denominada pharming, deviene del avance del conocimiento informático y de la programación web, y es la forma en la que diversas páginas web pueden ser copiadas, clonadas prácticamente al 100% o en algunas de sus características claves, para así inducir al error a los clientes de estas empresas. Esto sumado a la facilidad que existe hoy en día para adquirir espacios y dominios en la web.

El phishing posee casi en su totalidad todas las características de un delito informático, puesto que como mencionamos anteriormente para su cometimiento no hace falta la presencia o cercanía física del delincuente con la víctima o el sistema o equipo que se tenga por objetivo. El enorme tránsito que existe en la web provoca que prácticamente que todos sus usuarios sean víctimas potenciales de este delito, puesto que un solo criminal a un clic de distancia puede afectar o intentar afectar a una o hasta cientos de miles de personas a la vez, con un gasto de recursos mínimo y un potencial retorno incuantificable.

Estas características antes mencionadas provocan que este tipo de modalidad de apropiación fraudulenta por medios electrónicos sea muy complicada de castigar por el derecho penal; puesto que la identificación del sujeto activo considerando que no hay un nexo material entre la víctima y el victimario y que los mismos pueden ser cometidos desde distintas partes del mundo, el hallar indicios o evidencia que nos direcciona a un culpable es muy complicado, considerando también la volatilidad de la información que está alojada en la red. (Delgado & Sanchez, 2022)

Actualmente en la legislación ecuatoriana el delito de phishing no está abarcado únicamente por la normativa penal, sino que también el legislador castiga también mediante leyes de protección de datos, el acceso no consentido a datos de información de carácter personal, aunque para el presente estudio lo relevante de la conducta radica en la apropiación patrimonial, es importante hacer énfasis en este inciso puesto que es una característica relevante que posee Ecuador a la hora de normar el delito de apropiación fraudulenta por medios electrónicos. (Hernández, 2023)

Considerando las conductas descritas en el COIP la manipulación, alteración o modificación, de un sistema informático incluye también las modalidades de espionaje y sabotaje informático. Sobre estas modalidades recae la particularidad que la normativa vigente los recoge en artículos específicos, sin embargo como mencionamos anteriormente esto no debería sorprendernos puesto que los delitos informáticos pueden poseer uno o varios de los bienes jurídicos protegidos. (Pino S. A., 2015)

Esto quiere decir que para el objeto de esta investigación el hacking informático o espionaje no se considera un fin; puesto que el fin de estas conductas es la obtención de datos personales o protegidos sino que se considera un medio mediante el cual el criminal enviará la información obtenida para provocar un daño en patrimonio ajeno, es decir que considerando la teoría penal estas modalidades forman parte del presupuesto que puede estar contenido o enmarcado dentro del delito que estamos estudiando.

Sobre estas modalidades descritas la doctrina se encuentra en continuo debate acerca de la aproximación más cercana que tienen con los delitos comunes como la estafa, puesto que cumple con los presupuestos establecidos por la normativa en el aspecto de que a través del engaño buscan inducir al error a la víctima para conseguir un beneficio patrimonial. El punto de debate aquí se genera sobre la consideración del aspecto psicológico en la inducción al engaño y error que algunos autores consideran que tiene que estar presente, mismo que en los delitos informáticos no figuran puesto que el delito se comete a través de un medio no mediante contacto personal. Es decir, que los delitos cometidos a través de medios digitales, no pueden considerarse en esa esfera puesto que no existe la manipulación de sujeto a sujeto, es más bien; en términos coloquiales, como ir de pesca, lanzar muchos cebos y ver quién pica. (Torres, 2022)

Proceso de identificación del sujeto activo del delito

Para la identificación del sujeto activo y posterior imputación de la pena en los delitos penales, los ordenamientos jurídicos en concordancia con sus normativas constitucionales y de Derechos Humanos establecen procedimientos a seguir en primera instancia para comprobar que la conducta que tenemos en frente, puede ser considerada o no un delito, y los posibles implicados o autores materiales e intelectuales de la misma.

Proceso penal ecuatoriano

El proceso penal ecuatoriano, está descrito a lo largo del C.O.I.P. y en general está compuesto por dos etapas, una pre penal y la otra encaminada a conformar o reunir los requisitos necesarios para conseguir una pena sobre un determinado sujeto a causa de una conducta tipificada.

La etapa pre penal está conformada principalmente por la etapa de instrucción fiscal, esta etapa empieza en cuanto el fiscal; quién es el dueño de la acción penal en estos casos, conoce del hecho. Esto puede darse; según nuestro Código Orgánico Integral Penal, de las siguientes maneras; a partir de una denuncia, en la que cualquier ciudadano puede acusar el cometimiento de una

infracción ante la Fiscalía General o Policía Nacional, o personal del Sistema integral o autoridad referente al ámbito del tránsito. Los que directamente pondrán de inmediato en conocimiento de la Fiscalía. Así mismo puede darse por la suscripción de informes de supervisión, dichos informes son efectuados por organismos de control como la Contraloría General, mismos que, de encontrar irregularidades deberán ser enviados a la Fiscalía. Por último, a través de providencias judiciales, esto es, todos los autos y sentencias emitidos por las o los jueces o tribunales que tengan un interés penal. (Asamblea Nacional, 2014, pág. 220)

Una vez en conocimiento del fiscal, empieza el proceso de investigación previa, que tiene como objetivo en primer lugar, establecer que el hecho frente al que nos encontramos corresponda a una conducta tipificada en la ley como delito. Esta etapa del proceso busca recoger indicios sobre cómo se llevó a cabo el hecho y sus motivos, así como la también intenta establecer nexos entre los indicios con posibles sospechosos de haber participado en el hecho investigado, para esto, el fiscal tiene entre uno o dos años, según la pena que contemple el delito investigado y en el caso de desaparición de personas, no se puede cerrar hasta que aparezca, o los indicios recogidos sirvan para establecer un imputado por el delito que se considere.

Una vez terminada esta etapa y certificada la existencia de un delito penal, empieza la denominada etapa de instrucción fiscal, en la que los sospechosos de tener participación en el mismo son llamados al proceso de formulación de cargos en el cuál la fiscalía como ellos tienen la oportunidad de presentar sus alegatos y pruebas con el fin de convencer al juzgador de formular o no cargos en contra de los sospechosos.

En base a la temática de este estudio, que se basa principalmente en los mecanismos que posee la norma para identificar el sujeto activo, estas dos etapas son las primordiales a tener en cuenta. El proceso penal en Ecuador culmina con la audiencia preparatoria de juicio y posterior juicio, en donde se imputa una pena en caso de establecerse responsabilidades o no. (Asamblea Nacional, 2014)

Criminalística

La rama de la ciencia penal encargada de la recolección de indicios y evidencias, para el esclarecimiento y sanción de hechos delictivos sean estos en el mundo material o informático es la Criminalística. La palabra Criminalística proviene del latín CRIME e INIS, que significa delito grave, así como de los sufijos griegos ISTA e ICA que significa ocupación u oficio. (Ochoa, 2007)

Historia

Con la evolución de la investigación de los delitos para apoyar al sistema judicial en la obtención de evidencias, pruebas, indicios que permitan una mejor aplicación de la justicia cuando antes primaba principalmente la declaración del testigo, hubieron muchos tratadistas que con un criterio estrecho pretendían que la Criminalista debía ser parte del Derecho Penal, conformado por normativa o leyes, o de la Criminología que se encarga de entender las causas y formas del fenómeno criminal, mientras la Criminalística estudia, verifica, examina y analiza vestigios, indicios y evidencias. De acuerdo a este simple análisis, necesariamente la Criminalística requiere el tratamiento de ciencia que se le da en la actualidad.

La Criminalística es la ciencia de carácter empírico e interdisciplinario que, mediante la integración de diversos métodos y técnicas, estudia, verifica, examina y analiza vestigios, indicios y evidencias de toda índole y origen, en y/o dejados por cualquier individuo, organismo u objeto a efectos de determinar las circunstancias, medios e individuos implicados en el hecho que dio lugar a su estudio e intervención. (Zapana, 2012)

Básicamente la criminalística, es una ciencia que presta los elementos necesarios para la investigación de los delitos de la índole que fuera, incluido los delitos informáticos.

Por la inseguridad que vivimos actualmente en el país, la criminalística cobra gran importancia ya que es una herramienta que permite la investigación de los

delitos en términos generales, que cada día son más frecuentes y que causan grave perjuicio a los bienes de propiedad de las personas víctimas de este delito. En este panorama de inseguridad, hay un mayor auge de los delitos informáticos, lo que ha obligado a desarrollar elementos que permitan enfrentar la investigación de los delitos informáticos, que por su complejidad, como ya ha sido analizado demanda una investigación exhaustiva y contar con peritos muy bien capacitados para constituirse en un elemento que permita castigar a quienes incurren en el cometimiento del tipo de delitos que nos ocupa.

La criminalística aplicada a los delitos cometidos a través de medios informáticos

Con el avance tecnológico y la utilización de medios digitales en el cometimiento de delitos de toda índole, robo, secuestros, asesinatos, pedofilia, etc., y, en aquellos que son específicamente delitos electrónicos, denominados como tales por enmarcarse dentro de las características enlistadas para ellos, esto ha obligado a que los informáticos permanentemente estén desarrollando herramientas que les permita brindar mayor seguridad a los sistemas, redes, páginas web, internet, etc., y precautelar los bienes de las potenciales víctimas.

Paralelamente los sistemas creados por el personal informático para dar mayor seguridad, también han sido utilizados como herramientas en la investigación de los delitos electrónicos, ya que permiten establecer las vulneraciones a los sistemas, rastros de borrado de información, cambio de configuraciones, ingreso de los usuarios al sistema, manipulación de los sistemas en beneficio de terceros, etc.

Las técnicas forenses digitales, son una rama de las Ciencias Forenses y Miguel López Delgado la define como todos los principios y técnicas que conforman los procesos de identificación, levantamiento, conservación, registro detallado, procesamiento y análisis; y presentación de evidencias digitales y que según su pertinencia las mismas puedan ser aceptadas legalmente en un proceso judicial. (Delgado M. L., 2007)

Con el cometimiento cada vez más frecuente de delitos informáticos, por la vulneración de la seguridad de los equipos y sistemas, ha traído aparejado el surgimiento de las técnicas forense digitales, son herramientas que se utilizan tanto en la investigación de los delitos comunes, en los cuales se evidencia un delito informático de manera concurrente y en la investigación de los delitos informáticos.

Las técnicas forenses digitales se constituyen en un puntal importante para la justicia en la solución o determinación de responsables del cometimiento de delitos informáticos, ya que por las características propias de este tipo de delito, no se configuran con tanta facilidad los elementos que permitan su esclarecimiento y estos deben ser encontrados basándose principalmente en los conocimientos de quienes son los peritos asignados a su investigación, de ello dependerá en gran medida los resultados que permita dar con los responsables.

Sin duda en los países desarrollados se trabaja desde hace muchos años, en desarrollar esta área de las ciencias forenses, podemos encontrar en la página de la Interpol en referencia al análisis forense digital:

El objetivo principal del análisis forense digital es extraer datos contenidos en pruebas electrónicas, transformarlos en información de utilidad operativa y presentar las conclusiones con miras a la persecución penal. En todas las fases del proceso se utilizan avanzadas técnicas forenses, a fin de que las conclusiones resulten admisibles ante un tribunal. (Interpol, 2023)

Lo cual nos permite entender con toda claridad el objetivo de la forense digital.

Al momento de ejecutarla, se debe tener presente lo señalado por Darío A. Piccirilli (2022), aspectos que permitirán obtener los resultados que puedan conducir al castigo de los responsables del delito investigado:

1. El perfil del problema o del delito a peritar
2. El procedimiento científico a aplicar

3. La presencia de peritos de parte
4. El procedimiento protocolar a aplicar, en relación a la situación procesal
5. Las herramientas de forense informática a aplicar o la combinación de más de una herramienta
6. La posibilidad de nuevas pruebas
7. La posibilidad de aclarar los puntos de pericia requeridos por el Juez que interviene en la causa
8. La existencia de cadena de custodia de la prueba informática
9. Las condiciones en que la prueba ha sido preservada. (La Forensia como Herramienta en la Pericia Informática, 2022)

Las recomendaciones aquí listadas, para el cuidado de la recolección de evidencias en los entornos digitales son nada más que una guía general de la manera de trabajar, sin embargo cada ordenamiento jurídico tiene sus propias consideraciones acerca del sistema probatorio sus reglas y aproximaciones hacía el entorno digital.

Indicios y evidencias en el entorno digital

Reglas del manejo de evidencia en el entorno digital en Ecuador.

Los procesos criminalísticos que se llevan a cabo al momento de tener conocimiento del cometimiento de un delito, son de vital importancia para el desarrollo del proceso final. Métodos como la Inspección Ocular Técnica, toma y análisis de muestras, se emplean generalmente en la mayoría de delitos estipulados en el C.O.I.P. en Ecuador. Sin embargo, en la esfera de los delitos que requieran la recolección de indicios o evidencia en el entorno digital se emplean mecanismos distintos en la fase investigativa.

Así tenemos como en la Sección Primera del C.O.I.P. acerca de las actuaciones especiales de investigación, encontramos las técnicas que generalmente se llevarán a cabo en delitos que empleen medios informáticos.

Así tenemos en primer lugar, la retención de correspondencia, esta técnica de investigación amplió sus reglas para abarcar no solo la correspondencia física sino también la electrónica. Sobre esto nuestra norma penal vigente manifiesta que la retención, apertura y examen de la correspondencia y otros documentos se tomara en cuenta que la correspondencia electrónica o de cualquier tipo o medio de comunicación, es de carácter inviolable, excepto los casos expresamente autorizados por la Constitución de la República y el COIP. Solo el juzgador podrá, previa solicitud en apego a la garantía de motivación autorizar al fiscal, para retener, abrir y revisar y analizar la correspondencia, siempre y cuando exista suficiente evidencia para dar por hecho que la misma podría tener alguna información relevante para el proceso de investigación. Para realizar la apertura y examen de la misma y los elementos que puedan tener relación con los hechos y de la infracción investigada y sus autores o participantes, se deberá notificar a la persona interesada y ya sea que este comparezca o no, se procederá a leer la correspondencia de manera reservada, informando de la pericia a la víctima y al acusado o a su abogado defensor sea público o privado. En caso de que a la diligencia faltaren por cualquier motivo las partes, la misma se podrá realizar ante testigos. siempre considerando que todos los participantes de la misma realizar un juramento de reserva. Si la correspondencia investigada se encuentra efectivamente relacionada con el hecho investigado, se agregará inmediatamente al expediente fiscal; o en caso de no resultar útiles, se deben devolver al sitio de donde fueron tomados o al propietario. Si se encontrare en la diligencia alguna escritura en clave o en un idioma distinto, se puede solicitar la inmediata traducción a los peritos especializados. (Código Orgánico Integral Penal, 2014, págs. 179-180)

Este mecanismo se emplea especialmente cuando los delitos implican el correo electrónico como medio para acceder a datos que procuren la apropiación fraudulenta del patrimonio de la víctima.

Además de este sistema, el COIP en su artículo 476, prevé la forma en la que; en caso que sea necesario, se interceptarán comunicaciones y datos informáticos. En general para llevar a cabo la interceptación de datos

informáticos, el fiscal que lleva el caso, debe presentar solicitud motivada frente al juez quien en caso de ser necesario otorgará un plazo de 90 días para este procedimiento. En caso de ser aceptada la interceptación, de la información obtenida sólo se podrá emplear lo relativo al caso en cuestión. De esta técnica investigativa se excluyen la población protegida como los niños y adolescentes.

La prueba

Luego de las pericias llevadas a cabo por los peritos en el ámbito criminalístico y la ciencia forense en el campo digital, las evidencias encontradas son valoradas por las partes del proceso para que de acuerdo a su criterio, puedan ser empleadas o no en el proceso de juicio. La prueba tiene como fin sustentar frente al juez la existencia de un hecho y sus responsables, por ende deben observar una serie de requisitos para considerar su validez. En el terreno de los delitos que emplean un sistema informático como medio, los tipos de indicios y evidencias que pueden ser detectados son variables, y en muchos casos escasos, puesto que como se ha comentado con anterioridad, en este tipo de delitos no existe el nexo de cercanía física entre el criminal y la víctima, y los medios informáticos suelen ser altamente manipulables, por lo que las pruebas para este tipo de delitos suele ser muy especial y sensible.

Reglas probatorias aplicadas al ámbito digital en Ecuador.

Los delitos que emplean sistemas informáticos para su materialización, como es lógico de asumir, requieren para su etapa probatoria de la utilización de pruebas digitales, para esto los ordenamientos jurídicos han ido adaptando sus normativas ante este escenario y en concordancia del respeto de las garantías que cada país ofrece a sus procesados.

En Ecuador, la prueba digital, conforme a lo establecido, es considerada como un tipo de prueba documental, por lo que se rige a los lineamientos establecidos para este tipo de pruebas además de que la propia norma contiene lineamientos especiales para esta, tal como lo establece el Artículo 500 del Código orgánico Integral Penal acerca del contenido digital que señala que el contenido digital es todo acto que representa hechos,

información o conceptos propios de la realidad, que se encuentre almacenados, o hayan sido procesados o transmitidos a través de cualquier medio tecnológico o informático, incluidos los programas diseñados con un fin o para una entidad específica, o que se encuentre interconectado o relacionado uno o varios entre sí. Por último señala que en el proceso de investigación será importante considerar que el análisis, la valoración, la recuperación y así también la presentación del contenido de tipo digital que se almacene en dispositivos o medios informáticos se realizará mediante técnicas forenses orientadas al tipo digital. Que, cuando dicho contenido se encuentre almacenado en memorias volátiles, otros dispositivos de almacenamiento o equipos de tecnología que por su naturaleza hagan parte de la infraestructura esencial del sector público o privado, se realizará la pericia correspondiente en el lugar, en tiempo real, con las técnicas digitales forenses que garanticen la preservación de la integridad de los mismos, además se aplicarán los preceptos de cadena de custodia facilitando su posterior valoración y análisis. Cuando el contenido de tipo digital que se busque levantar para su posterior procesamiento se encuentre contenido en medios no volátiles, se realizará su recolección, con técnicas digitales forenses para preservar su integridad, se aplicará la cadena de custodia y se facilitará su posterior valoración y análisis de contenido. Cuando lo recolectado sea el medio físico que se emplee para un fin dentro de un sistema digital durante una investigación, registro o en su defecto allanamiento, se debe identificar y almacenar siguiendo el inventario estipulado para este tipo de objetos, fijando la ubicación física del mismo con fotografías del mismo y del lugar donde se encontró, protegiéndolo a través de técnicas forenses en medios de almacenamiento adecuados para su traslado mediante cadena de custodia a los centros de acopio temporales o permanentes especializados para este fin. (Asamblea Nacional, 2014, pág. 190)

Por último, la normativa ecuatoriana obliga que al hacer uso de la respectiva prueba digital la misma vaya acompañada del testimonio del perito especializado que dé cuenta de cómo se obtuvo, las técnicas periciales aplicadas y la veracidad de las mismas.

Problemas para la persecución del sujeto activo en los delitos informáticos

En el desarrollo del presente marco teórico se han ido mencionando distintas problemáticas que enfrenta el derecho penal al enfocarse en esta corriente de delitos que emplean como medio sistemas informáticos. Muchas de estas situaciones son el motivo principal para que estos delitos en su gran mayoría no sean denunciados, o en el caso de serlo, no logren conseguir la imputación de un culpable.

Territorialidad de los delitos informáticos.

En los delitos informáticos se enfrenta un problema particular, que es el relativo a la territorialidad de estos, ya que como se ha venido analizando suele ocurrir que quienes cometen la infracción se encuentran fuera del país en el que se afecta la propiedad de los bienes de la víctima o víctimas. Los delitos comunes tienen como particularidad que se establece con toda claridad, el sitio donde se comete o la escena del crimen y consecuentemente se puede establecer sin duda que autoridad tiene la competencia para Investigarlo y Juzgarlo..

Establecer el territorio en el cual se cometió el delito, se puede determinar luego del análisis de las pruebas, indicios o rastros que el delincuente haya dejado en los equipos, sistemas o redes que utilizó al cometerlo, ya que en primera instancia no se puede determinar.

Por lo expuesto, se puede colegir que investigar el ciberdelito es complejo y se requiere que quienes intervengan cuenten con los conocimientos, herramientas y agudeza, para llegar a establecer el sitio donde físicamente se ejecutó el delito, que tiene su víctima generalmente en otro país, lo cual dificulta la investigación, seguimiento y detención de los delincuentes digitales, ya que las autoridades tienen jurisdicción determinada por la ley y consecuentemente no pueden realizar el proceso de investigación sin contar con la colaboración de las autoridades de otros países donde se tiene indicios podría físicamente encontrarse el agresor.

La colaboración entre países amparados en las leyes, convenios o acuerdos vigentes, es lo que se requiere para llevar a término los procesos de

investigación y juzgamiento, el cual debe ser en el lugar donde se encuentre la víctima de este hecho delictivo.

Ubicar a un delincuente digital tiene su grado de dificultad, ya que generalmente son expertos en informática y conocen perfectamente las formas de camuflar o de ocultar en la red su ubicación, ya que enmascaran su ubicación haciendo que los rastros digitales señalen que la conexión es con servidores de otros países y no del país donde él se encuentra, lo cual hace de la investigación un recorrido tortuoso donde se debe ir descartando cuales son los indicios enmascarados y cuales son indicios válidos para la ubicación definitiva del delincuente.

El ciberdelincuente como hemos indicado, usa sus conocimientos para camuflar su actividad y ubicación, utilizando una variedad de recursos que le da cierta ventaja para esconder sus huellas y ponerse a buen recaudo, aunque es innegable que no hay crimen perfecto, y el delito digital tiene sus aristas pero también tiene un rastro del recorrido realizado de la señal en la red, que aunque sea difícil de rastrear no es imposible y de hecho la solución de casos de relieve internacional así nos permiten confirmarlo.

El delito informático a diferencia de otros delitos que son realizados por personas con o sin conocimientos profesionales, este es, generalmente realizado por personas o redes con amplio y basto conocimiento en esta materia, única garantía de poder obtener los resultados favorables a sus intereses. Esta característica del delincuente digital, tiene como consecuencia que aquellos que hacen la investigación, peritos y criminalistas, deban ser profesionales que permanentemente estén actualizando sus conocimientos y capacitándose, lo que debe garantizar que los resultados en la investigación conduzcan a determinar la responsabilidad del delito cometido.

Determinar el territorio o país en el cual se inició el cometimiento del delito digital, determina también la jurisdicción y competencia de las Autoridades que les corresponde investigar y juzgar a los responsables.

Por lo tanto en jurisdicción y competencia en materia penal informática y al desconocerse el lugar de procedencia del ilícito, debe aplicarse la jurisdicción de lugar de los bienes jurídicos afectados hasta hallar la

procedencia a través de medios e investigaciones informáticas que den con el paradero del ataque in situ. (Espinosa, 2014)

Medios en los que se almacena la información digital

Dentro de las normativas procesales, como se mencionaba anteriormente, para la vinculación de un sujeto a un hecho delictivo para posteriormente conseguir una pena, se deben conseguir y evaluar indicios, evidencia, para que luego el titular de dicha acción pueda emplearlos como medios probatorios durante el proceso jurisdiccional. En un proceso tradicional encontraremos medios de prueba más o menos contundentes, y en diversas presentaciones y provenientes de diversas fuentes; como podrían ser el ADN, la huella digital, pericias documentológicas, etc.

En el caso de los delitos informáticos, mucha o gran parte de la evidencia que los operadores de justicia e investigadores deben buscar para su procesamiento y poder ser utilizados como prueba, se encuentran en el mundo digital, ya sea en sistemas de almacenamiento privados, o de instituciones obligadas a almacenar datos relativos al tráfico de internet de sus usuarios. Esto despierta una problemática que contiene dos esferas consideradas para este estudio.

La primera, los medios de almacenamiento de información, en el ámbito informático pueden llegar a ser muy volubles y manipulables, según el tipo de información que almacenen y sus características físicas. El formateo por ejemplo de un disco duro de una computadora común, está al alcance de unos pocos clics, de igual manera en sistemas mucho más pequeños. Así mismo, cuando estos delitos se comenten en grandes instituciones públicas o privadas, la información puede estar contenida en equipos que no pueden parar de funcionar o que son muy delicados para el funcionamiento de las entidades. Es por esto que la labor de los peritos de criminalística dedicados a este tipo de delitos es trascendental, puesto que tienen la obligación de realizar una evaluación integral del contexto para garantizar que información que pueda ser útil para un proceso penal pueda ser resguardada y no sea manipulada.

Ahora bien, el almacenamiento así como todos los demás elementos informáticos también ha evolucionado, es así que es muy común a día de hoy que empresas e incluso usuarios comunes, empleen los denominados servidores en la nube. Al respecto de este tipo de servidores, los mismos vuelven mucho más complicado el que hacer de los peritos expertos para obtención de dichos datos, puesto que en los casos de que no se pueda acceder directamente a la información, la misma debe ser solicitado a quién fuere el titular de dichos servicios, que comúnmente no instalan sus servidores en nuestro país. (Lamperti, 2014)

Anonimidad en internet

El internet, como medio de comunicación en continuo avance y desarrollo, tanto desde el aspecto positivo como negativa, va creando distintas herramientas que pueden ser muy útiles y otras tantas que a pesar de resultar útiles, pueden ser empleadas para el cometimiento de crímenes.

Así tenemos que entre la problemática del tratamiento de los delitos cometidos en medios informáticos esta la posibilidad cierta de pasar desapercibidos al momento de actuar, al menos hasta cierto nivel de tecnología. El internet y sus operados han ido desarrollando distintas formas para enmascarar datos relevantes de los usuarios de internet como las direcciones IP, mismos que se han puesto de moda entre los usuarios comunes del internet para acceder a contenido digital que está disponible fuera de los límites del territorio en el que habitan, conocidos como VPN o red virtual privada. Así mismo se puede conseguir estos fines empleando navegadores orientados a guardar la anonimidad como lo son TOR o Freenet. (Lamperti, 2014)

Así mismo, y continuando con la idea de la facilidad de encubrir la identidad de los usuarios en internet, otra de las problemáticas más recurrentes en los servicios informáticos, es la facilidad de suplantar la identidad de un tercero, misma a la que se puede acceder mediante una de las modalidades del delitos objeto de este estudio como es el phishing o mediante la clonación de dicho usuario.

Incidencia del delito de apropiación fraudulenta por medios informáticos

La incidencia de este delito a nivel regional y global, sufrió un crecimiento exponencial y muy fuerte debido al fenómeno vivido durante la pandemia por COVID 19, mismo que obligó el traslado al mundo virtual a un sin número de actividades que regularmente no se desarrollaban ahí, así como provocó que muchas más personas aprendiesen a operar medios informáticos o simplemente que deban buscar obtener acceso al internet por diversos motivos. Ante esto, la consecuencia lógica, es el crecimiento estadístico de la presencia de los delitos informáticos en general, y particularmente el que nos atañe en esta investigación.

Ecuador

En el caso ecuatoriano, el delito tipificado como apropiación fraudulenta por medio electrónicos, se encuentra tipificado en el Código Orgánico Integral Penal vigente, y alcanza penas que van de 1 a 3 años; según información publicada por la Fiscalía General del Estado, en el 2021 se registraron 3962 denuncias específicamente acerca de este delito. Al respecto del repunte histórico del mismo, en 2020 se presentaron apenas 2280 casos, es decir, en menos de un año la ocurrencia de este delito en Ecuador creció un 73,7%, dicha tendencia de aumento de casos viene en alza desde 2017, aunque en menor porcentaje; siendo únicamente antecedido por el delito de estafa, del cual se han presentado 16,272 denuncias en 2021, aunque es preciso señalar que el delito de estafa posee un carácter específico en el que se considera delito electrónico, mismo que no está especificado dentro del número señalado. (Ciberdelitos, 2021)

Para poder interpretar de mejor manera este hecho, y precisamente realizando un enfoque hacia la identificación del sujeto activo del delito y su consecuente sanción mediante el proceso penal, es menester indicar que, según datos estadísticas de la Fiscalía General del Estado, hasta la finalización del 2021, únicamente un 2,7% de los casos impulsados por esta entidad se encuentran en etapa de juicio, y únicamente 12 de los mismos han alcanzado una sanción y se encuentran en etapa de impugnación, y el 90,8% no ha

superado aún el proceso de investigación previa. Esta información estadística es de carácter general y contiene todos los delitos sancionados por nuestra normativa penal, sin embargo, es alarmante la consideración problemática que conlleva llevar los procesos penales a su fin en Ecuador.

Colombia

El caso colombiano, es un caso para el que en primer lugar hay que hacer una precisión referente a este delito, esto es que el mismo tiene otra tipificación muy distinta a la establecida por la normativa ecuatoriana. En Colombia la apropiación fraudulenta por medios electrónicos se configura mediante dos delitos de acuerdo al Código Penal Colombiano (2000), el primero hace referencia al hurto calificado a nivel general en todas sus formas posibles para sancionar. En la parte más específica se hace referencia a la esfera de apropiación, si lo comparamos con la normativa ecuatoriana, sin mencionar específicamente el medio a través del cual se materialice la conducta descrita, siendo que esta especificidad se encuentra en el siguiente artículo del mismo código. El artículo 269 I, agrega a los elementos que pueden conformar el hurto, el cometimiento del mismo a través de medios informáticos o similares, e indica que sancionará la conducta que se oriente a vulnerar las seguridades informáticas con el fin de buscar una apropiación de tipo ilegítima mediante la alteración o manipulación de los mencionados sistemas, suplantación de usuario en el mundo digital o frente a sistema de autenticación. Las penas señaladas para este delito pueden ser a 14 años. (Senado de la República de Colombia, 2000, pág. 214)

De esta forma observamos como hacen uso de un nuevo artículo para complementar y añadir esferas al delito de hurto tradicional, y se equipara al que hace de los delitos electrónicos, además de los tradicionales. Esta normativa es la más cercana al delito normado en la ley ecuatoriana en cuanto a la conducta que castiga y el medio a través del cual se comete, es decir la apropiación patrimonial de tipo fraudulenta mediante el uso de medios o herramientas informáticas.

Ahora bien, considerando lo anteriormente expuesto, en términos estadísticos, el caso colombiano sigue la misma suerte que Ecuador. El delito

de hurto en su modalidad perpetrada mediante medios electrónicos, ocupa el tercer lugar en crecimiento durante el año 2021, únicamente adelantado por los delitos de violación de datos personales y el acceso abusivo a sistemas informáticos. A pesar de ocupar el tercer lugar en porcentaje de ocurrencia en comparación al período anterior, este delito ocupa el primer lugar en número de casos presentados con un total de 17,608 denuncias, siendo el delito con más perpetrado en el país colombiano. (Garcia, 2022)

Perú

En el caso del Perú, el delito de buscar el provecho ilícito en detrimento de un tercero mediante el uso de herramientas informáticas está tipificado por la Ley de Delitos Informáticos o Ley No. 30096 (2014) que en su artículo 8 manifiesta que todo aquel de manera deliberada e ilegítima procure para sí o para un tercero un beneficio ilícito en detrimento de un tercero mediante el acto de diseñar, introducir, alterar, borrar, suprimir o clonar datos de tipo informático o cualquier tipo de interferencia o manipulación que tenga como objetivo alterar el funcionamiento de un sistema informático, será sancionado con una pena privativa de libertad que no puede ser menor a tres ni mayor que ocho años y con sesenta hasta los ciento veinte días de multa. Así mismo consideran que la pena de privación de libertad no puede ser menor de cinco ni mayor a diez años y además de ochenta hasta ciento cuarenta días de multa cuando el afectado sea el Estado y su patrimonio, cuanto este sea el que se encuentra destinado a fines asistenciales o proyectos de apoyo social. (Congreso de la República de Perú, 2014, pág. 5)

Este artículo contiene la conducta más similar a la tipificada en la normativa ecuatoriana. En cuanto al factor estadístico, el auge de los mismos es evidente, ocupando el delito señalado el primer lugar en índice de ocurrencia en relación a los demás delitos informáticos tipificados, con un total de 10924 de denuncias. Este número representa un crecimiento del 57,2% en relación con las 6946 denuncias recibidas en 2020. En pro de la virtud de identificar el sujeto activo de este delito, el titular de la acción penal peruana ha solicitado 36 pedidos conservación de activos a distintos servidores con la colaboración de varios países y así mismo Perú ha recibido este pedido en dos ocasiones

durante 2021, provenientes de Argentina y República Checa; por lo que se evidencia una cooperación internacional activa para la persecución de esta conducta. (Medina, 2022)

España

En España, el caso de las defraudaciones a través de medios electrónicos tiene un panorama normativo un tanto distinto que los países previamente mencionados, mismo que es relevante para obtener una visión general y un poco más global de la incidencia de esta conducta en comparación con lo que sucede en Ecuador. En la normativa penal española, esta conducta está directamente incluida en el delito de estafa, siendo considerada como una modalidad más de este delito. Al respecto diversos tratadistas han manifestado la necesidad de tener un articulado autónomo, sin embargo en la práctica ha logrado solventar diversos vacíos legales que poseía la norma previo a su implementación en 1995. (García-Cervigón, 2008)

Al respecto de la estadística recogida en el período del año 2021 en consideración de esta conducta, el fraude informático ocupa el primer lugar en índice de casos conocidos por la justicia española entre los demás delitos informáticos tipificados, alcanzando un total de 267011 hechos conocidos, mismo que ocupa el 87,4% del total de hechos conocidos relacionados con cibercriminalidad. De este número mencionado sin embargo, se agregan otras estadísticas en cuanto al avance de los procesos acorde a los hechos conocidos, es así que tenemos que de los mismos se han logrado esclarecer 46141 hechos, y solamente en 13801 se han producido detenidos o individualizado investigados. (Gutierrez, y otros, 2022)

Mecanismos de cooperación internacional

Ante el surgimiento de nuevos fenómenos jurídicos, la comunidad global emplea diversos mecanismos para intentar combatir mancomunadamente a los mismos, o en su defecto lograr una organización global más efectiva, como ha ocurrido con convenios de derechos humanos, o sobre propiedad intelectual; el caso de los delitos electrónicos con todas sus características especiales no tiene por qué ser distinto, al ser un fenómeno jurídico técnicamente reciente, los convenios y tratados internacionales al respecto aún se encuentran en

proceso de refinamiento, o aún cuentan con limitado suscriptores a los mismos, pero sin embargo existen varios de gran importancia que abordaremos a continuación.

Convenio de Budapest

De entre varios convenios existentes de cooperación en distintos temas del índole del derecho penal en relación a lo delitos informáticos, uno de los más relevantes es el Convenio sobre la Cibercriminalidad alcanzado en Budapest, durante el Consejo Europeo. Dicho convenio se empezó a construir a partir del año 1983, por la recomendación de conocedores del tema acerca de la necesidad de crear un parámetro común para definir este tipo de delitos. La creación del convenio se alargó hasta el 8 de noviembre de 2001, cuando fue recibió finalmente su aprobación. (Gómez, 2010)

El convenio de Budapest, busca que se realicen ajustes en los ordenamientos jurídicos de los países suscriptores y adoptar las distintas definiciones y términos empleados en el mismo, esto con la finalidad de contar con un marco jurídico común para conseguir elevar la efectividad para el combate de estos delitos. El convenio en su objetivo de equiparar y regular los delitos electrónicos, establece cuatro categorías para los mismos, mismas que son los referente a la confidencialidad, los orientados a proteger la integridad y los dispuestos en pro de garantizar la disponibilidad de los datos y además sistemas informáticos. Así también agregan los delitos informáticos, los delitos que tienen que ver con el contenido y los delitos en cuanto a las infracciones a la propiedad intelectual y los derecho afines. (Council of Europe, 2001)

Con la evolución del mismo se han ido agregando nuevos apartados al convenio, como en 2003 se agregó el protocolo que busca regular temas de racismo y xenofobia por medios informáticos. (Toledo & Cruz, 2020)

Hablando netamente de su estructura, a breves rasgos el Convenio está dividido en cuatro capítulos. En el primer capítulo se define y explica la terminología que se empleará a lo largo del Convenio también conocido como de Budapest, de entre lo más destacado encontramos las definiciones que extenderán a continuación.

Sobre los sistemas informáticos, el convenio lo define como todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, que entre sus funciones, o la de alguno de los elementos que la componen, sea el tratamiento de tipo automático de datos durante la ejecución de dicho programa. Por datos informáticos, establecen entender que son todas las representaciones de hechos, informaciones o conceptos que se expresen de cualquier forma que sea susceptible de darle un tratamiento informático, incluyendo en este apartado los programas creados para que un sistema realice una función específica. Al proveedor de servicios lo definen como todas las entidades sea que fueren de naturaleza pública o privada, que oferte a sus usuario el servicio de comunicación mediante un sistema informático, y además a las entidades que se dediquen al procesamiento y almacenamiento de dichos datos de tipo informático para garantizar el servicio de comunicación o como un servicio para sus usuarios. Y por último, acerca de los datos que se creen mediante el tráfico de comunicaciones informáticas, se considerarán a todos los relativos a las comunicaciones efectuadas a través de un sistema informático, que se haya generado por este y forme parte de la cadena comunicacional, entre estos consideramos los que indiquen su origen, el destino de la comunicación, la ruta seguida, la hora y fecha, así como cuanto tiempo duró dicha comunicación. (Council of Europe, 2001, pág. 4)

El segundo capítulo del convenio establece las disposiciones, recomendando la forma de definir las conductas que se buscan regular mismas que se organizan en las categorías señaladas previamente, es así que en relación al tema central de esta investigación tenemos que en la categoría de Delitos Informáticos el Convenio recomienda sobre la apropiación fraudulenta por medio de un sistema informático que quienes formen parte de dicho convenio deben considerar la adopción a través de su normativa la tipificación del delito en su normativa interna, de los actos que realizados deliberadamente produzcan un perjuicio de tipo patrimonial a un tercero, mediante el mal uso o alteración de datos informáticos o la interferencia a un sistema con la intención de arrojar daño y obtener un beneficio económico. (Council of Europe, 2001)

La segunda sección de este capítulo, complementa esta tipificación de los delitos informáticos a través de la definición de mecanismo procesales sugeridos a adoptar por los firmantes del convenios. Medidas entre las que encontramos las forma de conservación de datos informáticos almacenados, su registro y confiscación, así mismo las normas para la obtención en tiempo real de esta información. Por último, en su tercer capítulo el Convenio abarca las formas de cooperación internacional, asistencia mutua y herramientas como la extradición. Y en su cuarto capitulo establece disposiciones finales que incluyen detalles de la conformación del mismo. (Díaz, 2021)

La Relación del Ecuador con el Convenio de Budapest.

Ecuador a día de hoy aún no ha completado el proceso de adhesión a este convenio, puesto que el mismo debe seguir un trámite complejo, que abarca desde la modificación normativa hacía una que se adecue a lo establecido en el Convenio; sin embargo, en este proceso de adhesión que empezó alrededor del año 2008, se han hecho diversos avances al respecto, es así que el 4 de abril de 2022, el propio Consejo de Europa, en su portal web publica lo siguiente:

Ecuador fue invitado el 30 de marzo de 2022 a adherirse al Convenio de Budapest sobre Ciberdelincuencia. Por lo tanto, 81 Estados son ahora Partes (66), lo han firmado o han sido invitados a adherirse (15).

Las autoridades de Ecuador han estado cooperando con el Consejo de Europa en materia de delitos cibernéticos en múltiples ocasiones, comenzando en 2008, cuando la Organización de Estados Americanos y el Consejo de Europa coorganizaron un taller regional sobre delitos cibernéticos para países de América Latina celebrado en Colombia. . En 2020/2021, esto condujo a reformas del derecho penal que alinearon en términos generales la legislación nacional con los artículos de derecho penal sustantivo del Convenio de Budapest sobre Delito Cibernético. (Council of Europe Portal, 2022)

A decir de la Fiscalía General del estado, la necesidad de contar con este tipo de instrumentos es imperante, y por esto desde su competencia han

impulsado la coordinación con Ministerio de Gobierno y Cancillería en conjunto con el Consejo de Europa para realizar un análisis de la normativa ecuatoriana para realizar recomendaciones a la Asamblea Nacional con el fin de adaptar nuestra normativa a los requerimientos del Convenio; así mismo han avanzado con la creación de la Unidad Especializada contra la Ciberdelincuencia.

Como último elemento acerca de la vinculación del Convenio de Budapest con nuestro país, es muy importante abordar el tema de la extradición, que no es otra cosa que la entrega de una persona detenida en un país a otro que mediante el proceso determinado por su legislación la reclamara para seguir en su contra un proceso acusatorio. Al respecto nuestra Constitución vigente señala que en ningún caso se concederá la extradición de una ecuatoriana o ecuatoriano. Su juzgamiento se sujetará a las leyes del Ecuador. (Constitución de la República del Ecuador, 2008) Sin embargo, para el convenio estudiado guarda especial relevancia, por las características transnacionales de los delitos informáticos por lo que le dedica un apartado especial dentro del mismo, en donde entre otras cosas establece que, la extradición aplicará cuando las legislaciones castiguen la misma conducta delictiva y sobre esta pese una pena privativa de libertad de mínimo un año o mayor, además establece reglas a seguir cuando la extradición en este tipo de delitos se choque con otros tratados firmados por alguno de los países involucrados, sin embargo menciona que la extradición se someterá a las normas de derecho interno de cada país. (Convenio sobre la Ciberdelincuencia, 2001)

En nuestra consideración, y como se abordará más adelante, la figura de la extradición tal y como está planteada en nuestra normativa, es decir completamente denegada, puede generar inconvenientes a la hora de someterse a estos convenios internacionales en términos de la cooperación que como nación podemos dar para la persecución de estas conductas así como de la que podemos recibir.

La Relación de Latinoamérica con el Convenio de Budapest.

En Latinoamérica, la adhesión a dicho Convenio ha avanzado a pasos lentos, aunque a través de diversos organismos regionales se ha promovido su adhesión, es así que a día de hoy los únicos países latinos en ser parte del Convenio son Argentina, Chile, Colombia, Costa Rica, Cuba, El Salvador, Perú y Panamá.

En el caso argentino, la adhesión al convenio se realizó aun cuando el mismo no encontraba del todo de la aprobación mayoritario puesto que lo consideraron por mucho tiempo ambiguo, dejando de lado las disposiciones relacionadas con medidas acerca de la jurisdicción y pornografía infantil.

Siguiendo por la misma línea, Chile, se adhirió al convenio en 2017, presentando reservas similares a las del caso argentino, sobre todo en el tema jurisdiccional en cuanto a guardarse la salvedad de no prestar colaboración en caso de delitos no tipificados en su normativa.

Colombia, suscribió la entrada en vigor del convenio en 2020, en el caso colombiano se guardaron reservas en torno a la recolección de datos en tiempo real, considerando que al tener una normativa en torno a los datos personales y privacidad, se aplicaría dicha normativa y no la establecida en este apartado del convenio.

La Convención de la Organización de las Naciones Unidas para el combate de la Delincuencia Organizada Transnacional

De más está redundar acerca de las características territoriales especiales que posee el delito de apropiación fraudulenta a través de medios electrónicos. Y que los entornos digitales y la criminalidad que los ataca, guardan características propias de organizaciones criminales que perpetran delitos más tradicionales, es por esto que la Organización de las Naciones Unidas persiguió la suscripción de la Convención contra la delincuencia organizada transnacional.

Esta convención, ratificada por 147 estados signatarios, sirve como marco procedimental para la prosecución de la delincuencia organizada transnacional, que comúnmente conocemos en delitos como el lavado de

activos, la corrupción, narcotráfico, etc. Pero el mismo también guarda cierta amplitud en cuanto a las conductas a castigar, y dentro de esta se ha enmarcado a las infracciones de tipo informático, siempre que estas fueren cometidas por una organización. Esta convención también abre las puertas a los estados para conseguir de forma más sencilla vías de capacitación en la lucha contra estos delitos.

Elac 2018

En Latinoamérica , los organismos regionales han venido trabajando por impulsar la integración regional en el mundo digital, que, aunque no se hayan desarrollado convenios tan específicos como el anteriormente revisado, diversas reuniones han fijado metas y objetivos por conseguir a nivel regional.

La Comisión Económica para América Latina y el Caribe, en adelante CEPAL, a través del eLAC 2018 La revolución digital, definió las metas para la región enfocadas en primer lugar en la economía, dejando un apartado especial para estudiar el efecto de los ciberdelitos en la economía digital. Al respecto el documento señala:

Los costos de los ciberdelitos ascendieron a 113.000 millones de dólares en 2013, según datos de Symantec para países del mundo. Esos costos habrían alcanzado los 8.000 millones de dólares en el Brasil, seguido de México con 3.000 millones y Colombia con 464 millones. El número de personas afectadas por este tipo de delito en todo el mundo fue del orden de 378 millones, con un costo promedio por víctima de 298 dólares, lo que representa un aumento del 50% respecto de los 197 dólares de 2012. El 83% de los costos directos fueron causados por fraudes, reparaciones, robos y pérdidas. (La nueva revolución digital, De la Internet del consumo a la Internet de la producción, 2015)

De los datos señalados, es lógico suponer que si a las fechas de la publicación se manejaban cifras que llamaban la atención, en la actualidad las mismas deben haber crecido exponencialmente, en conjunto con el número de usuarios con acceso a internet y las nuevas formas de delitos. Para tener una

visión más clara de las actividades ilícitas realizadas en el período de tiempo determinado en el documento de la CEPAL, el mismo señala:

(...)el 50% de los usuarios fueron víctimas de la ciberdelincuencia o de situaciones negativas en línea —por ejemplo, recibir imágenes de cuerpos desnudos de personas desconocidas o ser intimidados o acosados— y el 41% fueron víctimas de ataques de programas maliciosos (malware), virus, estafas, fraudes y robos.(...) (La nueva revolución digital, De la Internet del consumo a la Internet de la producción, 2015)

Al respecto el documento suscrito plantea la necesidad de coordinación transfronteriza, señalando la importancia de los países de suscribirse al Convenio de Budapest por las áreas relevantes en las que se activa. Además señalan que a pesar de que la legislación en la materia ha avanzado, aún no se encuentra armonizada del todo entre los países miembros de la región.

Interpol

La Interpol es una organización de carácter internacional, dedicada a la cooperación policial internacional fundada en 1914, de la cual Ecuador hace parte. Sus fines en general se centran en colaborar con las organizaciones de policía de los países miembros facilitando la comunicación y el intercambio de información, pero también el apoyo técnico. (Institute, s.f.)

En este sentido, esta organización pone a disposición de sus miembros también la preparación en distintos ámbitos de la delincuencia informática, es así que cuenta con capacitación para optimizar el uso de pruebas electrónicas por ejemplo. Ofreciendo apoyo operativo, orientación, capacitación y la vinculación a sus laboratorios forenses especializados en materia digital. Así mismo también han establecido directrices para la conformación de laboratorios para estos fines, y guías para conformar una primera intervención criminalística de los delitos informáticos de manera adecuada. (Interpol, s.f.)

Tratados de cooperación jurídica internacional

Tratado de Medellín.

Los tratados de cooperación jurídica internacional, son de carácter general, no abarcan como tal un tipo de delito en específico como podrían ser los informáticos, pero si funcionan de acuerdo a sus características como herramientas fundamentales para su procesamiento. Es así que el Tratado de Medellín o Tratado Relativo a la Transmisión Electrónica de Solicitudes de Cooperación Jurídica Internacional entre Autoridades Centrales, se suscribió con la finalidad de aprovechar la plataforma informática denominada Iber@, la misma que funciona como una vía de comunicación segura, confidencial y directa para la transmisión instantánea de solicitudes de cooperación; evitando el tiempo que ocuparía enviar dichas solicitudes por los canales pertinentes de tipo físico. (Tratado de Medellín: Un avance desde Iberoamérica para el mundo, 2023)

Convención Interamericana sobre Asistencia Mutua en Materia Penal.

Otro de los tratados de especial importancia para el Ecuador, es el de asistencia mutua de materia penal, creado en 1992 y ratificado por el Ecuador en 2001. Es una de las herramientas más importantes para los operadores de justicia del país, ratificada por 25 estados, tiene como objetivos ser el siguiente paso evolutivo de los tratados bilaterales a multilaterales, evadir el proceso de trámite diplomático que suponía la solicitud de asistencia y la elaboración de un marco común para dicha asistencia. Es así que para su funcionamiento se designan autoridades centrales en los distintos estados partícipes para facilitar la comunicación mutua para llevar a cabo la asistencia mutua en materia penal. Para un efectivo funcionamiento de esta convención la misma emplea redes de comunicación como la Red Hemisférica de Intercambio de Información para la Asistencia Mutua en Materia Penal y Extradición y la Red Iberoamericana de Cooperación Jurídica Internacional, IberRed. (Instructivo de Cooperación Penal Internacional, 2006)

METODOLOGÍA DE LA INVESTIGACIÓN
CAPÍTULO II

Metodología de la Investigación

Enfoque de la Investigación

Para el presente trabajo de investigación es necesario definir el tipo de enfoque metodológico a seguir. En consideración de su naturaleza y el problema jurídico que abarca, el enfoque que guio la estructuración tanto del plano teórico como argumentativa, fue el enfoque cualitativo.

La determinación del uso de este enfoque se basa en que el mismo se emplea para el análisis de una realidad subjetiva, contrastando la interpretación de dicha realidad con los resultados del estudio de la misma mediante distintas fuentes bibliográficas y documentación disponible. Este enfoque además tiene un carácter flexible, que nos permitirá reconducir la información de ser necesario, así como incluir en ella el máximo de diversidad posible para alcanzar una interpretación de la realidad, que, aunque subjetiva, sirva como referencia para entender el problema jurídico abordado.

En el caso del presente trabajo de investigación se contrastará la determinación teórica del delito de apropiación fraudulenta a través de medios informáticos, con el marco normativo local, la problemática jurídica que plantea la doctrina para el estudio de este tipo de delitos, y el enfoque que se le ha dado en cuerpos normativos de otros estados así como la incidencia que ha alcanzado el mismo. De esta manera pretendemos obtener un mejor punto de vista acerca de la problemática jurídica planteada, para determinar las dificultades que deben ser superadas, específicamente por el ordenamiento jurídico ecuatoriano.

Método de la investigación

Descriptiva

El método elegido para esta investigación es el método descriptivo, este método de investigación busca, como su nombre lo indica, describir un fenómeno o realidad concreta, buscando evidenciar sus características tal y cómo se presentan en la realidad, sin intentar manipular la información, sino buscando únicamente comprender los elementos objetos de la investigación.

Este tipo de método de investigación es el más empleado al momento de estudiar un fenómeno social, en este caso el estudio del delito de apropiación fraudulenta por medios informáticos, además de contener en su naturaleza una discusión netamente jurídica; tiene una incidencia social en continuo crecimiento, debido al auge de los casos conocidos así como de la evidente dificultad de los estados para tratarlos, estas características son las que pensamos extraer a través de recopilación de datos e información proveniente de fuentes doctrinarias y de las administraciones públicas para dar forma al presente trabajo.

Explicativa

Se empleará además este tipo de método de investigación, puesto que como se mencionaba previamente, se espera, además de comprender la problemática jurídica, concluir en por qué existen distintas formas de abordarla y que situaciones determinan estas diferencias y problemáticas particulares; yendo un poco más allá de únicamente describir la realidad sino estudiar sus motivos para ampliar la forma de comprender la problemática que plantean los delitos cometidos a través de medios informáticos.

Período y Lugar de la Investigación

Para el presente trabajo de investigación, se han determinado límites espacio temporales enfocados en el órgano jurisdiccional ecuatoriano, en el período del año 2021; considerando la realidad social vivida en dicho período que provocó un auge notorio en la criminalidad a través de medios informáticos.

Universo y Muestra de la Investigación

Universo.

El universo de este proyecto de investigación es el territorio nacional del Ecuador, en el 77% de la población que posee acceso al internet y tecnologías de la información, es decir alrededor de 13,6 millones de usuarios.

Muestra.

Los casos 3962 casos denunciados del delito de apropiación fraudulenta a través de medios electrónicos.

Procesamiento y análisis de la información

En el transcurso de esta investigación, se recopiló información proveniente de fuentes doctrinarias y oficiales que gozan de ser fiables, la misma se ha organizado de manera que se pueda comprender la problemática jurídica abordada desde su origen conceptual primario, hasta lo específico del mismo y los diversos puntos de vista que lo han ido moldeando.

Para esta investigación ha sido crucial contar con fuentes de información estadística, para evidenciar en un primer lugar, el porqué de la relevancia de este estudio basado en la creciente incidencia de este tipo de delitos, más en el contexto social vivido debido a la pandemia, en donde la gran parte de nuestras actividades se trasladaron a entornos digitales, para esto se han empleado fuentes oficiales de los sistemas de justicia así como trabajos de investigación previos que han plasmado esta información.

Por el carácter jurídico de esta investigación, se han incluido en el marco teórico referencial no solamente diversas fuentes doctrinarias, sino también enfoque previos y criterios estandarizados mediante convenios internacionales, etc. Para esto se ha analizado la jurisprudencia encontrada, las normas jurídicas vigentes en Ecuador y otros estados que consideramos relevantes para la construir una comparativa válida que sirva como referencia.

Para complementar la información compartida acerca del tema de esta investigación, se realizará un análisis de una sentencia de primera instancia en relación al delito estudiando, para reconocer de manera estructurada los elementos que lo componen.

ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS
CAPÍTULO III

Análisis e interpretación de los resultados.

Análisis del proceso penal No. 01613201700483

El presente proceso obedece al procedimiento de los procesos de acción penal pública, en donde actúan el Fiscal General del Estado, el Sr. Homer Eliceo Mogrovejo y la señora Ruth León Guerrero; en adelante accionantes, en contra de la Sra. Iñiguez Álvarez Verónica Daniela, en adelante procesada, a quién se la causa del cometimiento del delito de apropiación fraudulenta por medios electrónicos.

Hechos.

Del proceso penal No. 01613201700483 se desprende lo siguiente en relación a los hechos descritos por Fiscalía:

La señorita Verónica Daniela Iñiguez Álvarez se desempeñaba en calidad de JEFA DE AGENCIA DE LA COOPERATIVA COOPERA que funcionaba en este cantón Santa Isabel , en fecha 28 de Octubre de 2012 a las 15h53 minutos se genera en el sistema informático de Coopera en Santa Isabel una Nota de crédito Préstamo de socio por la cantidad de seis mil dólares americanos que es realizado bajo la observación “N/C contra factura de ganado” por el usuario Nro.127 que pertenecía a la señorita Verónica Daniela Iñiguez y se deposita en la cuenta de ahorros de HOMER ELICEO MOGROVEJO ABRIL y este mismo día a las 15h57:58 minutos se registra el retiro de la base de datos de los 6.000 dólares, cuya transacción fue realizada a través del usuario 252 perteneciente a Edgar Ordoñez un cajero de Coopera en Santa Isabel; pero no se encuentra la papeleta de retiro ni la impresión de la Nota de Crédito firmadas por el socio a nombre de quien se carga el préstamo el señor HOMER ELICEO MOGROVEJO ABRIL, este nunca firmó ningún documento que le haga responsable del crédito ya que el crédito realizado por él fue de veinte mil dólares en fechas anteriores y que ya fueron canceladas, y que esta es una nueva transacción sin documentación física de respaldo, Y una vez Como se descubre esto, el señor Mogrovejo solicita a la Cooperativa se levante la

hipoteca que pesa sobre un bien inmueble de su propiedad se da cuenta que debía seis mil dólares adicionales que se encontraban cargados en su cuenta, él manifiesta que nunca retiró el dinero, quien realizó esta transacción es Verónica Iñiguez ya que ella como jefa de Agencia es la única que tenía acceso a la bóveda para sacar el dinero en la cantidad que se señala, y no tenía acceso Edgar Ordoñez el jefe de caja, únicamente utilizó su clave que ella lo conocía para simular un retiro través de este cajero, por lo tanto manipula el medio informático de la cooperativa para tomar los 6.000.00 que lo carga a Homer Mogrovejo que es un familiar cercano a ella inclusive. Además era la única autorizada para hacer los créditos, por su calidad de jefa de agencia.
(2017)

De lo descrito en el dictamen acusatorio de la Fiscalía, y en relación al delito objeto de esta investigación, se presume en esta etapa que la procesada en uso de su posición privilegiada dentro de la Cooperativa mencionada, vulneró los sistemas informáticos de la misma, en primer lugar para realizar un préstamo ficticio y segundo para recuperar ese dinero de la cuenta del cliente donde fue depositado. Esto se adecua a la conducta sancionable descrita por el delito de apropiación fraudulenta por medios electrónicos.

Pericias informáticas como elementos de convicción.

Del proceso penal No. 01613201700483 se desprende lo siguiente en relación a las pericias informáticas realizadas:

A fojas 669 el informe realizado por el perito informático que se verifica que existe el sistema informático ORACLE y que en el este sistema se encuentra registrado el préstamo para al señor Romel Mogrovejo. Además tenemos un cuadro en que realiza el reporte de transacciones.
(2017)

En el presente proceso se solicitó pericia informática, en la que se identificó los softwares que emplea la cooperativa afectada, obteniendo acceso a los mismos para emitir reporte de transacciones y de los movimientos presuntamente realizados por la procesada para la materialización del delito

siguiendo la normativa vigente para prueba pericial en relación a los delitos informáticos, esto es la participación del perito experto en el proceso de manera testimonial para fundamentar las pericias realizadas y las conclusiones extraídas de la misma. La forma en la que se recogió la prueba se adecua a las reglas determinadas para la prueba digital en los casos que las mismas se encuentren en equipos tecnológicos que forman parte de la infraestructura del sector privado, realizando una recolección en tiempo real para preservar la integridad de la información.

Resolución.

En el presente proceso y una vez ventiladas todas sus etapas, el juez competente para conocer la causa declaro culpable a la procesada en calidad de autora y responsable.

Análisis.

Para concluir con el presente análisis, de este proceso podemos rescatar diversos elementos que se han venido exponiendo a lo largo de esta investigación, en primer lugar, la necesidad de tener una normativa adecuada en cuanto a los delitos informáticos se refiere, en este particular el proceso aquí citado empezó ventilándose mediante el Código Penal anterior, con la figura de apropiación ilícita que manifiesta:

Apropiación ilícita.- 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 utilizen 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. (Congreso Nacional del Ecuador, 2002)

Del que podríamos decir que es un adecuado antecesor a la normativa actual, misma que en su redacción especifica muchos más elementos propios

de los delitos cometidos a través de este tipo de sistemas. En el presente caso el juez consideró que al tratarse de conductas similares aplica el principio de favorabilidad, esto debido a que el código anterior fijaba una pena máxima de cinco años mientras que el vigente solo contempla sanciones de uno a tres años.

En segundo lugar, se evidencia la relevancia de contar con peritos expertos en sistemas informáticos, con el conocimiento adecuado en este ámbito que puedan sustentar adecuadamente su labor y realizar diligentemente y en apego a las normativas que reglan el mismo. En este tipo de procesos las pericias de expertos y lo que de ellas se pueda extraer juegan un papel probatoria muy relevante.

En tercer lugar, observamos las características de los sujetos activos clásicas de los delitos informáticos, esto es un individuo, con un conocimiento calificado en un sector, con una posición con la influencia y confianza adecuada para cometer esta conducta puesto que tiene acceso a todos los medios necesarios para llevarla adelante, elementos repetitivos en lo que a los delitos informáticos se refiere.

Y por último, y alejado del análisis centrado en el proceso penal, como señalábamos en los apartados anteriores de esta investigación, la identificación y sanción en los delitos penales en Ecuador adolece de una lentitud alarmante, situación que se contrapone a los características de diversos elementos de un delito informático, donde las pruebas, por ejemplo, son volubles y manipulables y muchas veces se necesita de un actuar eficaz de los órganos de justicia para acceder a las mismas.

Análisis del proceso por contravención No. 0928620146178

El presente proceso se considera relevante para el presente proyecto de investigación en el apartado de la figura de la responsabilidad por omisión, el presente caso cuenta ya con una condena en contra de tres individuos que, burlando las seguridades informáticas del Banco Pichincha accedieron a la cuenta de quién funge como actor de esta causa, para realizarse una transacción económica fraudulenta. El juez que conoció la causa la sancionó,

identificando a los autores materiales, sin embargo el propietario de la cuenta vulnerada decidió emprender un proceso en contra del Banco Pichincha, por considerar que no cumplió con las garantías mínimas de seguridad.

Hechos.

Del proceso se desprenden lo siguiente en relación a los hechos:

(...) desde hace algunos años mantiene un relación proveedor-usuario con el Banco Pichincha C. A, de los servicios que le proporciona, entre ellos, el servicio de claves electrónicas para transferencia de valores denominado “ Cash Management”. Para efectuar transacciones por este servicio, es necesario la posesión por parte del usuario del dispositivo denominado Token, que genera códigos numéricos que deben ser ingresados al momento de efectuar una transferencia, además del número de cédula del cliente y la clave de acceso a la banca electrónica. Que sin embargo de encontrarse en su poder el mencionado Token, con fecha 13 de julio del 2012, se registra una transferencia no autorizada de \$ 29.806,00, desde la cuenta corriente de su representada a la cuenta corriente No. 328043604 en el mismo Banco Pichincha, cuyo titular era el señor Juan Carlos Moncayo Valencia, quien posteriormente cerró la cuenta por decisión comercial, según información del mismo Banco. Ese mismo día, el Banco Pichincha, procedió a entregar de la misma cuenta, el cheque No. 763 por 15.000,00 y el cheque No. 765 por \$ 14.806,00 a nombre de Mario Sierra Merizalde y Gustavo Silva fuentes, respectivamente, en la Agencia del Banco Pichincha ubicada en el Centro Comercial Riocentro Los Ceibos, constituyéndose un gran perjuicio económico para su representada por la deficiencia en el servicio del Banco Pichincha. (2014)

De lo descrito se puede considerar que se podría configurar el delito objeto de esta investigación, puesto que tenemos en frente la vulneración de un sistema informático para la apropiación fraudulenta de un monto económico, sin embargo, por características que consideró el juzgador, decidió sancionarlo

con la figura de robo. Lo importante aquí viene por la demanda de contravención planteada por el actor por considerar que el Banco no ha prestado un servicio adecuado, esta demanda se basa en los siguientes hechos que se desprenden de las pericias realizadas.

Informes periciales.

Del proceso penal se desprende lo siguiente en relación a las pericias informáticas realizadas:

(...)en la experticia técnica realizada por la perito informática Mayra Arias Candelario, quien dice que la orden 9530238, fue cargada desde una dirección IP del Perú, que la transacción fue procesada exitosamente por el Banco, que ese mismo día hubieron veinticuatro registros de ingresos con el usuario del señor Vintimilla Rodas, de diferentes partes del mundo, Estonia, Australia, Estados Unidos, Ecuador, Perú, entre otros, Perú desde donde salió la transferencia exitosa, que dos de los ingresos que hicieron de esa cuenta fueron de una región no identificada, que del registro de transferencia realizadas en los años 2009, 2010, 2011, 2012, 2013, 2014, 2015 y 2016, Austro Distribuciones solo registra dos usuarios con cédula de identidad claramente especificadas y una sola dirección IP, es decir, una sola es la máquina habitual con las que se han realizado las transacciones a lo largo de todo estos años, la dirección IP 186429894, ubicada en Salcedo- Ecuador, no en Perú, no en Estados Unidos, no en Estonia, ni en ninguna otra parte. Esta información está avalada en el informe de la Superintendencia de Bancos, en el Oficio No. DNAE- SAU del 2013, No. 05724, mientras que la dirección IP que está ubicada en Lima Perú de donde salió la transacción exitosa, avalada por el Banco Pichincha, es una dirección de IP que registra eventos fraudulentos y a pesar de todos esos veinticuatro ingresos a la cuenta ese mismo día de diferentes partes del mundo y a pesar que de la dirección IP ya registraba evento

fraudulento, del Banco Pichincha no saltaron ninguna sola alarma, no hubo ni siquiera una llamada al cliente. (2014)

Del presente informe pericial, es preciso señalar, la capacidad que se posee para el registro de actividades realizadas en el mundo digital. Y en relación a lo demandado, sirve como prueba de que el Banco acusado, no realizó un labor cuidadosa de prevención de riesgos, no considerando la serie de eventos sospechosos que se realizaron en un corto período de tiempo, ni brindando la posibilidad a su usuario de validar las transacciones aún tratándose de grandes montos.

Resolución.

La presente denuncia fue declarada con lugar, sentenciando al banco por prestar un servicio de tipo defectuoso amparado por la Ley orgánica de defensa del Consumidor.

Análisis.

En el presente proceso descrito lo fundamental, es observar el mecanismo señalado anteriormente que guarda relación con el delito estudiado, la responsabilidad por omisión. Y como a través de las pericias informáticas pertinentes se puede observar con facilidad si la entidad que funge como garante o guardia de un bien o información ha actuado diligentemente o el respeto del deber objetivo de cuidado. Si bien es cierto, a día de hoy las seguridades bancarias han avanzado notablemente, aún se registran muchos casos de delitos cometidos que tienen por objeto el acceso a elementos bancarios.

Análisis estadístico de la incidencia del delito de apropiación fraudulenta por medios electrónicos y similares

En la presente tabla se detalla la incidencia del delito objeto de este proyecto de investigación o similares a nivel de América del sur, y en el caso de España:

Tabla 1

Número de denuncias por país.

País	Artículo penal	Denuncias en 2021
Ecuador	COIP, Artículo 190.	1682
Colombia	Código Penal Colombiano, Artículo 269I.	17608
Perú	Ley de delitos informático, Artículo 8.	10924
Argentina	Código penal de la nación, Artículo 172.	330
Chile	LEY 21459, Artículo 7.	462
España	Ley Orgánica 10/1995, Artículo 249.	267011

Nota. Esta tabla establece número de hechos denunciados o procesados por país acerca del delito de apropiación fraudulenta por medios electrónicos o similares. Fuente: Autor.

De la estadística expuesta, se puede colegir fácilmente que el auge de este tipo de conductas delictivas está en pleno desarrollo, ocupando en varios casos el primer lugar dentro de los tipos penales denunciados en los diversos países señalados.

Sin embargo, de la misma también es preciso identificar las diferencias normativas entre cada país, en donde casos como el colombiano llama mucho la atención, por haberse incluido en la figura del hurto esta modalidad electrónica. Además en el caso de España se pone en evidencia la disputa doctrinaria mencionada previamente acerca de que si este tipo penal debe subsumirse o no dentro del delito propio de la estafa, ya que por sus diversas formas de materialización puede o no reunir todos los elementos conocidos de la estafa.

Por último, es menester de los estados a nivel regional e internacional, acoger las similitudes y diferencias presentes en cada uno de sus cuerpos normativos, para elaborar una hoja de ruta considerando que este tipo de delitos tienen alta probabilidad de reproducir sus afectaciones transnacionalmente.

Conclusiones

En consideración de los objetivos establecidos en el presente trabajo de investigación, podemos concluir que se ha logrado establecer de manera amplia y detallada el proceso de identificación de sujeto activo en el delito objeto del mismo, además mediante el uso de diversas fuentes bibliográficas se han abordado todos los elementos relativos al proceso de este tipo penal, abarcando las distintas concepciones del mismo, las características propias y particulares que posee y las diversas reglas que se han determinado para garantizar una tutela judicial efectiva en estos casos.

Así mismo, con el uso de fuentes estadísticas se ha podido esclarecer el panorama en cuanto a los delitos electrónicos a nivel de la región latinoamericana, encontrando como una constante el aumento vertiginoso del delito estudiado, incluso algún tiempo después del repunte que se dio durante la pandemia por el COVID 19; también esta revisión a nivel regional nos ha permitido conocer las formas distintas en las que se norma en otros países esta conducta, evidenciando formas de normarlo que la doctrina crítica por su ambigüedad o amplitud en muchos casos.

Por último, se estableció la importancia de contar con elementos comunes para el combate de este tipo de crímenes, puesto que por su naturaleza pueden influir en distintos países a la vez. Profundizando en sistemas bastante desarrollados como el Convenio para la Cibercriminalidad, y otros más específicos a nivel regional que se emplean en general para el tratamiento de delitos penales. Sobre las vías de mancomunidad, también hemos evidenciado la necesidad de ampliar lo normado acerca de la extradición, para conseguir vías de cooperación más ágiles y mejores.

Así podemos concluir que el delito de apropiación por medios electrónicos, es un delito que puede manifestarse en distintas formas y con diversas características, que como delito electrónico posee sus cualidades y dificultades para la sanción del mismo, que su incidencia seguirá en aumento, por cuanto los medios electrónicos son cada vez más comunes y que la

normativa relativa a los mismos, aún continúa en desarrollo y le queda bastante camino por recorrer.

Recomendaciones

Desde la comunidad jurídica en general, en cuanto a las cuestiones relativas a lo normativo se debe promover la finalización del proceso de adhesión de Ecuador al Convenio de Budapest, mismo que actualmente se encuentra en proceso.

En cuanto al órgano jurisdiccional y los elementos que lo componen, se debe promover la capacitación y constante actualización de jueces y fiscales en cuanto a los delitos electrónicos y sus particularidades y como se desarrollan y las diversas formas en las que se manifiestan.

En cuanto a los propietarios o titulares de sistemas informáticos que sirvan como guarda de patrimonio, información o derechos, los mismos deben establecer vías para mitigar los riesgos asociados a la cibercriminalidad en general, y fomentar mediante la comunicación el correcto uso de dichos sistemas.

En cuanto a la ciudadanía en general, y como observamos en el presente proyecto, los principales objetivos del delito de apropiación fraudulenta son los medios electrónicos que pueden comprometer el patrimonio, por lo que es necesario capacitarse en el correcto uso de los mismos, así como también acerca de como funcionan y en que modalidades se pueden presentar estos delitos, Y por último, es necesario reconocer las cláusulas de uso que poseen dichos medios electrónicos en cuanto a las obligaciones y deberes que poseen sus titulares para poder hacer valer sus derechos como usuarios.

Bibliografía

190 APROPIACIÓN FRAUDULENTO POR MEDIOS ELECTRÓNICOS, INC.1, 01613201700483 (UNIDAD JUDICIAL MULTICOMPETENTE DE SANTA ISABEL 12 de Septiembre de 2017).

Asamblea Constituyente. (2008). *Constitución de la República del Ecuador*. Registro Oficial 449. Obtenido de https://www.asambleanacional.gob.ec/sites/default/files/documents/old/constitucion_de_bolsillo.pdf

Asamblea Nacional. (2014). *Código Orgánico Integral Penal*. Quito. Obtenido de <https://www.asambleanacional.gob.ec/es/system/files/document.pdf>

Cabana, P. F. (2007). Los conceptos de manipulación informática y artificio semejante en el delito de estafa informática. *Eguzkilore*, 33-57.

Cantizano, M. G. (2012). Delincuencia informática en el ordenamiento jurídico penal peruano. *Gaceta Jurídica-N78B*, 69-72.

Caribe, C. E. (2015). *La nueva revolución digital, De la Internet del consumo a la Internet de la producción*. Santiago de Chile.

Cifuentes, S. G. (2021). *AUTORÍA Y PARTICIPACIÓN EN DELITOS DE OMISIÓN IMPROPIA: LA MASACRE*. Medellín.

Código Penal Español. (2023). Madrid.

Congreso de la República de Perú. (2014). *Ley de Delitos Informáticos*. Lima. Obtenido de [https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/C5F98BB564E5CCCF05258316006064AB/\\$FILE/6_Ley_30096.pdf](https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/C5F98BB564E5CCCF05258316006064AB/$FILE/6_Ley_30096.pdf)

Congreso Nacional de Chile. (2022). *LEY 21459*. Obtenido de <https://www.bcn.cl/leychile/navegar?idNorma=1177743>

Congreso Nacional del Ecuador. (2002). *Código Penal*. Quito. Obtenido de https://www.oas.org/juridico/PDFs/mesicic4_ecu_penal.pdf

- Council of Europe. (2001). *Convenio sobre la Ciberdelincuencia*. Budapest.
Obtenido de <https://rm.coe.int/16802fa403>
- Delgado, M. L. (2007). *Análisis Forense Digital*. España.
- Delgado, N. Y., & Sanchez, L. V. (2022). *Fraude informático en la modalidad de phishing y la necesaria actualización de la legislación para una eficiente persecución penal*. Pimentel.
- Díaz, C. D. (2021). *El Convenio de Budapest: Un análisis desde el ordenamiento jurídico colombiano*. Medellín.
- Espinosa, H. A. (2014). *El delito informático: Su evolución, punibilidad y proceso penal en Ecuador*. Quito.
- Estado, F. G. (2006). *Instructivo de Cooperación Penal Internacional*. Quito: Ediecuatorial.
- Estado, F. G. (2021). Ciberdelitos. *Perfil Criminológico*, 55-62.
- Feced, C. G. (2 de Febrero de 2023). *Business Insider*. Obtenido de Business Insider:
<https://www.businessinsider.es/negocio-ilegal-steve-jobs-steve-wozniak-apple-no-habria-existido-1192808>
- Fiscalía General del Estado. (08 de Octubre de 2020). *Fiscalía General del Estado*. Obtenido de
<https://www.fiscalia.gob.ec/fiscalia-abrio-instruccion-fiscal-contra-6-procesados-por-presunto-phishing/>
- Gallo, F. D. (2010). *Inseguridad Informática*. España.
- García, F. B. (2022). Comportamiento del ciberdelito en Colombia. *Tendencias del Cibercrimen 2021-2022*, 15-22.
- García-Cervigón, J. G. (2008). *El fraude informático en España e Italia. Tratamiento jurídico-penal y criminológico*. Madrid: Universidad Nacional de Educación a Distancia.

- Gómez, A. D. (2010). *El delito informática, su problemática y la cooperación internacional como paradigma de su solución: El convenio de Budapest*. La rioja: Redur.
- González, J. A., Meana, H. P., & López, P. G. (2015). Gusanos Informáticos. *Comunicaciones Libres*, 86.
- Gutierrez, J. L., JIMÉNEZ, F. S., SÁNCHEZ, D. H., MORENO, F. M., GARCÍA, M. R., ANA, M. V., . . . MARTÍN, M. A. (2022). *Informe sobre la cibercriminalidad en España*. España.
- Hernández, L. A. (2023). Delitos informáticos en Ecuador: Análisis de la intervención penal en casos de estafas mediante redes sociales. *Revista Científica Multidisciplinar G-Nerando*.
- INEC. (2022). *Tecnologías de la información y comunicación*. Quito.
- Institute, L. (s.f.). *Lisa Institute*. Obtenido de <https://www.lisainstitute.com/blogs/blog/interpol-funciones-como-trabajar>
- Interpol. (s.f.). Obtenido de <https://www.interpol.int/es/Como-trabajamos/Innovacion/Analisis-forense-digital>
- Interpol. (2023). *Interpol*. Obtenido de <https://www.interpol.int/es/Como-trabajamos/Innovacion/Analisis-forense-digital>
- Juan Carlos I. (1996). *Ley Orgánica 10/1995*. Obtenido de <https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444>
- Justicia, M. d. (1882). *Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal*. Madrid: Gaceta de Madrid.
- Lamperti, S. (2014). *Problemáticas en torno a la Investigación de delitos informáticos*. Castilla. Obtenido de https://www.researchgate.net/publication/324064192_Problematicas_en_torno_a_la_Investigacion_de_delitos_informaticos

- Leal, I. P. (2021). *Evolución histórica de la teoría del bien jurídico penal*. Corea del Sur: Universidad de Hankuk.
- Lux, L. M. (2017). El bien jurídico protegido en los delitos informáticos. *Revista Chilena de Derecho*.
- Machuca, L. (2012). *Los delitos Informáticos en la ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de datos y el principio de Seguridad Jurídica y Legalidad*. Ambato.
- Manjarres, I., & Jimenez, F. (2012). Caracterización de los delitos informáticos en Colombia. *Pensam.am*, 75-76.
- Medina, F. I. (2022). *Ciberdelincuencia*. Lima.
- Montenegro, D. B. (2015). El delito informático y su clasificación. *Revista de Ciencia, Tecnología e Innovación.*, 158-173.
- Ochoa, J. (2007). *La criminalística; la importancia dentro de la investigación penal; Caso Ecuatoriano*. Cuenca - Ecuador.
- Países, C. d. (12 de Junio de 2023). *Tratado de Medellín: Un avance desde Iberoamérica para el mundo*. Obtenido de Conferencia de los Ministros de Justicia de los Países:
<https://comjib.org/tratado-de-medellin-un-avance-desde-iberoamerica-para-el-mundo/>
- Pascual, A. (23 de abril de 2015). *El Confidencial*. Obtenido de https://www.elconfidencial.com/tecnologia/2011-10-22/hackers-cuando-la-curiosidad-te-lleva-a-la-carcel_773341/
- Piccirilli, D. A. (2022). *La Forensia como Herramienta en la Pericia Informática*. Buenos Aires: Universidad Nacional de La Plata.
- Pino, S. A. (2015). *Delitos Informáticos: Generalidades*. Quito: Oas.org.
- Pino, S. A. (2015). *Delitos Informáticos: Generalidades*. Quito: PUCE.
- Sain, G. (2015). Evolución histórica de los delitos informáticos. *Revista Pensamiento Penal*.

- Salgado, M., Robalino, J., & Pazmiño, L. (2021). Análisis conceptual del delito informático en Ecuador. *Revista Conrado*. Obtenido de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1990-86442021000100343
- Senado de la República de Colombia. (2000). *Código Penal Colombiano*. Bogota. Obtenido de https://oig.cepal.org/sites/default/files/2000_codigopenal_colombia.pdf
- Senado y Cámara de Diputados de la Nación Argentina. (1921). *CODIGO PENAL DE LA NACION*. Buenos Aires. Obtenido de <https://www.argentina.gob.ar/normativa/nacional/ley-11179-16546/texto>
- Strasbourg. (04 de abril de 2022). *Council of Europe Portal*. Obtenido de <https://www.coe.int/en/web/cybercrime/-/ecuador-invited-to-join-the-budapest-convention-on-cybercrime>
- Tiedemann, K. (1985). *Poder Económico y Delito*. España: Ariel.
- Toledo, I. N., & Cruz, L. V. (2020). *Herramientas del Convenio de Budapest sobre ciberdelincuencia, y su adecuación a la legislación nacional*. Santiago de Chile.
- Torres, M. P. (2022). *Delito de apropiación fraudulenta por medios electrónicos bajo la modalidad de phishing dentro del marco jurídico ecuatoriano*. Cuenca-Ecuador.
- Valencia, A. D. (2012). *La necesidad de Contemplar los delitos informáticos en el Código Penal del Estado de Michoacan*. Obtenido de Poder Judicial Michoacan: <https://www.poderjudicialmichoacan.gob.mx/tribunalm/biblioteca/almadeli a/indice.htm>
- Zambrano Mendieta, J., Dueñas Zambrano, K., & Macías Ordoñez, L. (2016). *Delito Informático. Procedimiento Penal en Ecuador. Dominio de las Ciencias*.
- Zapana, J. E. (2012). *La criminalística, hoy*. España.