UNIVERSIDAD INTERNACIONAL DEL ECUADOR

FACULTAD DE JURISPRUDENCIA, CIENCIAS SOCIALES Y HUMANIDADES
"ANDRÉS F. CORDOVA"

PROPUESTA DE INVESTIGACIÓN PREVIA A LA OBTENCIÓN DEL TÍTULO DE ABOGADO DE LOS TRIBUNALES Y JUZGADOS DEL ECUADOR

"IDENTIFICACIÓN DEL SUJETO ACTIVO EN EL DELITO DE ESTAFA A TRAVÉS DE MEDIOS DIGITALES Y ELECTRÓNICOS BAJO LA PERSPECTIVA DEL COIP EN EL ECUADOR''

AUTOR:

JUAN DIEGO GOMEZJURADO GOMEZJURADO

DIRECTOR:

LUIS FERNANDO SEMPÉRTEGUI FERNÁNDEZ

QUITO, DICIEMBRE 2022

RESUMEN Y PALABRAS CLAVE

Resumen

En la presente investigación analizaremos el procedimiento que maneja el Estado ecuatoriano para identificar el sujeto activo en el delito de estafa a través de medios digitales y electrónicos.

Con el ingreso de la tecnología en el desarrollo social, ha abierto las puertas a nuevos delitos que pueden ser realizados, causando una afectación en las personas que se encuentren utilizando el internet, uno de los delitos más frecuentes en la actualidad es la estafa a través de medios informáticos en la cual se ve afectado el patrimonio económico de las personas e incluso en varias ocasiones los datos personales.

Por lo tanto, analizaremos varios factores en los cuales podremos evidenciar si el procedimiento para identificar el sujeto activo en los delitos de estafa a través de medios electrónicos en el Ecuador es realmente eficaz.

Palabras clave

Estafa, medios electrónicos, autoría, ciberdelincuencia, procedimiento eficaz.

ABSTRACT AND KEY WORDS

ABSTRACT

In this research we will analyze the procedure used by the Ecuadorian State to identify the active subject in the crime of fraud through digital and electronic media.

With the entry of technology in social development, it has opened the doors to new crimes that can be carried out, causing an affectation in people who are using the internet, one of the most frequent crimes today is the fraud through computer media in which the economic heritage of people is affected and even on several occasions personal data.

Therefore, we will analyze several factors in which we will be able to demonstrate if the procedure to identify the active subject in the crimes of fraud through electronic media in Ecuador is effective.

KEY WORDS

Fraud, electronic media, authorship, cybercrime, effective procedure.

Índice

DECLARACIÓN DE AUTORÍA Y HONESTIDAD ACADÉMICA

Nombre: Juan Diego Gomezjurado Gomezjurado

Cédula de ciudadanía: 1724159767

Facultad: Jurisprudencia, Ciencias Sociales y Humanidades Andrés F. Córdova.

Escuela: Derecho

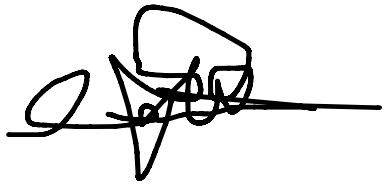
DECLARO QUE:

El trabajo de investigación de fin de carrera titulado ‘’Identificación del sujeto activo en el delito de estafa a través de medios digitales y electrónicos bajo la perspectiva del COIP en el Ecuador’’ para optar por el título de Abogado de los Tribunales y Juzgados del Ecuador, es de mi autoría exclusiva y producto de mi esfuerzo personal;

Las ideas, enunciaciones, citas de todo tipo e ilustraciones diversas; obtenidas de cualquier documento, obra, artículo, memoria, entre otros (versión impresa o digital), están citadas de forma clara y estricta, tanto en el cuerpo del texto como en la bibliografía.

Estoy plenamente informada de las sanciones universitarias y/o de otro orden en caso de falsedad de lo aquí declarado, en todo o en parte.

Quito, 24 de enero de 2023



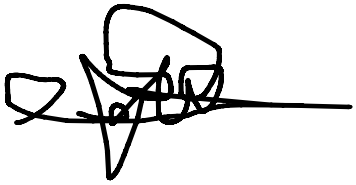
Juan Diego Gomezjurado Gomezjurado

AUTORIZACIÓN DE DERECHOS DE PROPIEDAD INTELECTUAL

Yo, Juan Diego Gomezjurado Gomezjurado, con cédula de identidad número 1724159767, en calidad de autor del trabajo de investigación ‘’Identificación del sujeto activo en el delito de estafa a través de medios digitales y electrónicos bajo la perspectiva del Código Orgánico Integral Penal en el Ecuador’’, autorizo a la Universidad Internacional del Ecuador (UIDE), a hacer uso de todos los contenidos que me pertenecen o de parte de los que contiene esta obra, con fines estrictamente académicos o de investigación.

Los derechos que como autor me corresponden, con excepción de la presente autorización, seguirán vigentes a mi favor, de conformidad con lo establecido en los artículos 5, 6, 8, 19 y demás pertinentes de la Ley de Propiedad Intelectual y su Reglamento en Ecuador.

Quito, 24 de enero de 2023



Juan Diego Gomezjurado Gomezjurado

AGRADECIMIENTOS

Quiero agradecer a mi mamá, quien ha hecho esfuerzos enormes para poder cumplir esta meta apoyándome de manera incondicional;

Agradezco a mi papá, el cual forjó mi carácter y mis valores para esforzarme por conseguir todo lo que me proponga y nunca rendirme;

Agradezco a mis abuelitas, Reina y Chelita, que con su amor, sus consejos y su apoyo me han impulsado y alentado para que me esfuerce y salga adelante;

Agradezco a mi enamorada, Carolyn Sánchez, por darme ese empujón cuando ya no quería avanzar, ayudándome y sobre todo estando en cada momento para lograr este objetivo;

Agradezco a mi tutor de tesis, Luis Sempértegui, quien admiro sus conocimientos y habilidades como abogado y docente, siendo siempre un modelo a seguir;

Agradezco al Dr. Gilberto Gutiérrez y al Dr. Fausto Vázquez, quienes han sido una inspiración para mí y han conseguido levantar mi espíritu del conocimiento y la abogacía;

Y finalmente, agradezco a toda la comunidad de la UIDE, a todos los docentes y autoridades de la facultad de derecho, quienes han estado siempre al pendiente apoyándome en cada paso para este logro.

DEDICATORIA

Quiero dedicar esta tesis a mi tutor, a mis familiares, mi enamorada, pero especialmente a mis abuelitas Reyna y Chelita, a mis abuelitos Efrén y Guillermo, y finalmente a mis Padres Diego y Alejandra quienes los amo con todo mi corazón y gracias por brindarme esta oportunidad de cumplir un sueño.

Introducción

En el presente estudio se plantea la investigación con un enfoque en el Código Orgánico Integral Penal (COIP) respecto a la identificación del sujeto activo en los delitos de estafa a través de medios electrónicos e informáticos, por lo cual se analizará el COIP y el proceso de juzgamiento del delito para poder reconocer la adecuación del tipo penal y cuál es el método investigativo en esta clase de delito.

Se complementará con un estudio doctrinario que permitirá entender a fondo como se ha desarrollado el proceso investigativo y normativo de la estafa electrónica en esta nueva era digital en el Ecuador y de igual manera examinar el proceso de indagación que han realizado otros países para poder combatir a los delincuentes informáticos responsables de la estafa a través de medios electrónicos.

En el año 2020, a raíz de la pandemia del COVID-19 existió un aumento en los casos de estafa a través de medios electrónicos, donde la mayoría no han llegado a dictaminar una sentencia ejecutoriada, estancándose hasta la etapa de investigación previa o incluso únicamente hasta la denuncia.

Cabe destacar que, la estafa a través de medios electrónicos surge a partir del origen de las redes y la tecnología, considerándolo un delito moderno con muchos aspectos técnicos por pulir a la luz del derecho penal, sin embargo, no se ha manejado una adecuación normativa y procesal de este crimen conforme lo ha detallado la doctrina, ocasionando así que el proceso de investigación y juzgamiento sea bastante ineficaz.

En el Ecuador, existen varias etapas para proceder con la investigación de un delito, pero el enfoque principal de esta es el trabajo investigativo que realiza fiscalía juntamente con criminalística, que en el caso de delitos cibernéticos trabajan las unidades especializadas conjuntamente.

El desarrollo fundamental y característico de este trabajo investigativo ha permitido evidenciar a través de las entrevistas realizadas a peritos de criminalística, que no se cuenta con el personal suficiente para poder abarcar todos los casos que surgen y por ende no se llega a juzgar a los autores responsables de este acto ilícito de estafa por medios digitales e informáticos.

Es importante resaltar que la ineficiencia no solamente proviene del trabajo de Fiscalía, también se necesita la cooperación de los ciudadanos, debido a que ellos tienen que colaborar con las indagaciones para poder recabar todos los elementos de convicción que permitan proceder con el juzgamiento del delito.

Ante todo lo expuesto, el objetivo de esta investigación es poder determinar si el Ecuador en su sistema normativo de juzgamiento, que actualmente es el COIP, se encuentra adecuado el delito de estafa a través de medios electrónicos e informáticos, conforme la doctrina lo ha establecido, con el fin de identificar eficazmente a los sujetos activos en esta clase de actos ilícitos, teniendo en cuenta que cada vez son crímenes más frecuentes, pero que llevan cierto grado de complejidad por motivo de que al delincuente no se la puede identificar físicamente desde un inicio.

Por ello, es de suma importancia realizar un estudio jurisprudencial y normativo para poder establecer e identificar si está correctamente adecuado el tipo penal, a la vez que se determine un protocolo de investigación especial para el proceso de señalamiento del autor del crimen, teniendo en cuenta que no se puede tratar de igual manera que otros delitos.

De tal modo, se hará énfasis en un estudio específico de jurisprudencia efectuado por el sistema penal ecuatoriano, para poder identificar el desarrollo de la investigación y el trabajo realizado por los agentes fiscales y peritos de criminalística, esto con el fin de analizar hasta que proceso de juzgamiento han llegado los casos y cuál es problema jurídico que enfrenta el sistema de justicia para poder determinar eficazmente a los sujetos activos en los delitos de estafa a través de medios electrónicos e informáticos.

Para esta investigación, se aplicará una metodología dogmática y de análisis de casos, con carácter cualitativo. Se utilizará una técnica de recolección documental y visitas a instituciones específicas acompañada de una comparación jurisprudencial, todo esto con el fin de esclarecer si existe un problema en el Ecuador a la hora de identificar a los sujetos activos en el delito de estafa a través de medios electrónicos e informáticos.

Para finalizar, acorde a todo lo expuesto, podremos analizar la evolución del proceso investigativo en el Ecuador respecto a este acto ilícito, donde finalmente se llegará a una conclusión que permitirá determinar cuál es la dificultad que enfrenta el sistema de justicia

ecuatoriano al momento de identificar eficazmente al sujeto activo en los delitos de estafa a través de medios electrónicos bajo la perspectiva del COIP.

Capítulo I

1. Marco Jurídico

1.1. Evolución y generalidades de los delitos electrónicos en la regulación jurídica del Ecuador

En la actualidad, nos encontramos en la era de la tecnología, y las personas se encuentran mayormente expuestas a todo el peligro que contiene internet, un mundo de descubrimientos interminables. Los delitos informáticos han trascendido y ahora existen delitos como el hacking, el daño a los datos o programas informáticos, el sabotaje informático, la interceptación no autorizada ya sea a través de objetos tecnológicos o un espionaje a través de la red, y de los varios que existen finalmente nos encontramos ante el más común ‘’la estafa a través de medios electrónicos’’ (Lara, 2014).

El sistema jurídico ecuatoriano cuenta con la tipificación del delito de estafa a través de medios electrónicos en su Código Orgánico Integral Penal (COIP); sin embargo, la primera vez que se tipificó este tipo de delito fue en el año 2002 en la Ley de Comercio Electrónico, Firmas y Mensaje[1] de texto, que por consiguiente fue adecuado al Código Penal, en esta ley podemos encontrar el delito de estafa a través de medio informáticos, pero lo interesante es que no se encuentra con tal nombre el delito, lo podemos identificar en el artículo 153 inciso 1 como apropiación ilícita (Liliana, 2020).

Si bien el tipo penal de delito de estafa a través de medios electrónicos se encuentra regulado desde el año 2002 en el Ecuador, este no es el verdadero problema que ha afrontado el sistema de justicia ecuatoriano.

En el año 2013 se incrementó la cantidad de quejas por parte de la ciudadanía, se reportaron varios casos de fraudes informáticos de los cuales la mayoría no pudo llegar a un procedimiento eficaz, y es ahí donde ha radicado el verdadero problema del Estado ecuatoriano, que cuenta con la tipificación del delito, pero no tiene el personal ni los recursos profesionales suficientes para poder

[1] Esta ley regula la contratación telemática, la prestación de servicios electrónicos, etc.; resguardando a los usuarios.

garantizar el procedimiento eficaz en la determinación del delito de estafa a través de medios electrónicos, permitiendo así la impunidad de los delincuentes cibernéticos (J., Bermeo, Villacreses, & Guerrero, 2018).

El Código Orgánico Integral Penal entró en vigor el 10 de febrero de 2014 y se mantiene vigente hasta la actualidad, dentro de él se encuentra tipificado el delito de estafa a través de medios electrónicos, a diferencia del Código Penal en el cual se encontraba como apropiación ilícita.

En el artículo 186 del COIP primero establece que la estafa es:

> *''Obtener para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años''.*

En los incisos 1 y 2 nos establece que la persona que:

> 1. Defraude mediante el uso de tarjeta de crédito, débito, pago o similares, cuando ella sea alterada, clonada, duplicada, hurtada, robada u obtenida sin legítimo consentimiento de su propietario.
>
> 2. Defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares.

Como podemos ver, en el COIP primero se establecen parámetros como la obtención de un beneficio patrimonial, el más común suele ser el patrimonio económico. En la tipificación de este delito, primero, lo adecua a una acción que tiene que ser realizada para poder ingresar dentro del tipo penal, por lo cual, es un delito de resultado, y posteriormente establece en los numerales 1 y 2 los requisitos para que tenga incidencia cuando son cometidos a través de medios informáticos, abarcando a la normativa, pero en el procedimiento se queda en un vacío que permite un perjuicio a los ciudadanos,

Ahora bien, la determinación del delito como pudimos observar es muy técnica, pero ¿cómo el COIP establece un procedimiento eficaz en la determinación del sujeto activo de este delito? Debemos tener en cuenta que nos encontramos ante un delito diferente al común (el que

causa conmoción dentro de la sociedad), los delitos a los que la sociedad está acostumbrado son los que se encuentra un delincuente de manera física.

En los delitos informáticos no tenemos una perspectiva real de quién es el delincuente, por ello, teniendo en cuenta que estamos en la era digital, se debería establecer un protocolo especial para este tipo de delitos, con el fin de garantizar la seguridad al ciudadano y, por otro lado, no dejar en impunidad los delitos.

Una evidencia clara que podemos obtener para evidenciar que el procedimiento en la identificación del autor del delito de estafa a través de medios electrónicos es ineficiente en el Ecuador, es el informe emitido por el diario El Universo el 08 de agosto de 2021, donde informó acerca de las siguientes cifras: En el 2020, la Fiscalía recibió 18.460 denuncias por estafa. Al 31 de julio del 2021, 16.763 continuaban en investigación previa, es decir, un 90 % de las querellas se encontraban en fase previa del proceso judicial.

Este problema parte de una falta de recursos prácticos y normativos por parte del sistema jurídico ecuatoriano el cual no es un problema actual, sino que viene acarreando desde el inicio de la implementación de tal delito.

Capítulo II

2. Análisis de los elementos del tipo penal de la estafa cometida por medios electrónicos

Para poder determinar que estamos ante un delito existen 4 pilares fundamentales que sostienen la base de la teoría del delito, estas son: conducta, tipicidad, antijuricidad, culpabilidad. Existen varias teorías alrededor de este análisis, sin embargo, vamos a partir de estos 4 elementos para analizar el tipo penal de la estafa cometida por medios electrónicos (Castillo R. B., 2018).

Como punto de partida debemos tener una conducta que se encuentre realizada por un sujeto activo, el cual es el actor de un hecho ilícito, es decir, quien realiza la conducta que al ser un delito de resultado se entiende que existe una voluntad por parte del actor, y esta conducta recae sobre un sujeto pasivo quien es la persona afectada.

El artículo 186 del COIP en su primer párrafo determina:

> *Art. 186. La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento*

de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera.

En este caso la conducta tendría que verse reflejada en que una persona obtenga un beneficio patrimonial engañando a otra a través de medios electrónicos como establece el inciso 2 o alterando, duplicando, clonando la tarjeta de la víctima tal como se encuentra establecido en el inciso 1.

De esta manera tendríamos un sujeto activo que realiza una conducta a un sujeto pasivo (víctima) y tiene una incidencia en el objeto material que sería la posesión del dinero y el objeto jurídico que sería el derecho patrimonial.

El sujeto activo que realiza un delito de estafa a través de medios electrónicos se lo identifica como cualquier persona con conocimientos del sistema informático, claro está que dentro del mundo digital se encuentra categorizado cada delincuente respecto a su nivel de conocimiento como los hackers[2], crackers[3] y phreakers[4], pesar de ello, sin importar cuál sea su nivel dentro del mundo informático, a la luz del COIP siempre va a ser el sujeto activo una persona natural o jurídica, de tal manera que no se deberá llegar únicamente al nombre de dominio o el protocolo de internet (IP) en el internet, se debe llegar a la persona que se encuentre de manera física a través del monitor o el sistema informático que esté utilizando (López, 2014).

La acción (conducta) que anteriormente fue analizada debe estar establecida en una norma o ley, esto se conoce como tipicidad, si la estafa no llega a ser consumada por medios electrónicos no recaería dentro de este tipo de delito del inciso 1 o 2, o si no existe un resultado del delito con beneficio patrimonial de igual modo no estaríamos dentro de esta falta.

Ahora, se discute que por el hecho de que se encuentre tipificado que debe ser una persona la que debe cometer el delito y dentro del mundo digital no se maneja esta terminología, por lo cual, no se debería responder por el resultado, pero utilizando la regla de la razón se sobreentiende

[2] Según la RAE, Hacker es: *Persona experta en alguna rama tecnológica que accede a un sistema informático o a informaciones ubicadas en dicho sistema o en la red de comunicaciones (bases de datos, programas informáticos, etc.) sin permiso del titular y sin necesidad de móvil o acción posterior alguna.*

[3] Según la RAE, Cracker es: *Persona que se dedica a entrar en sistemas informáticos de forma no autorizada e ilegal para conseguir información, perturbarlos, alterar su funcionamiento, inutilizarlos con fines dañinos u otros propósitos delictivos.*

[4] Phreakers: Son conocidos como piratas telefónicos que puede llegar a realizar actividades no autorizadas con los teléfonos, especialmente con los teléfonos inteligentes.

que una persona debe ser quien alteré o haya utilizado su cuerpo para manipular la tarjeta o el cajero electrónico.

La antijuricidad se entiende como un elemento valorativo que propone un análisis, una ponderación objetiva sobre el acto ilícito que fue realizado y el ordenamiento jurídico. Los delitos realizados a través de medios electrónicos deben ser antijurídicos porque lesionan los derechos constituidos en la Constitución, además de entender que el sujeto activo es una persona que tiene conocimiento pleno de manejo informático, causando un resultado directo con incidencia en el patrimonio (Cruz, 2016).

A la luz del COIP, para activar el elemento de culpabilidad la persona será penalmente responsable cuando sea imputable y actúe con conocimiento de la antijuricidad de su conducta, por lo cual, está claro desde un principio que el SA. del delito de estafa a través de medios electrónicos tiene el conocimiento suficiente para usar medios informáticos, por lo cual cumpliría con tal descripción y respecto a la imputabilidad existen causas que el COIP establece para eximir de la culpa a una persona, la cuales son las siguientes:

- Error de prohibición invencible y trastorno mental: Cuando la persona no puede prever la falta a la ley que causa su conducta, y cuando tiene un trastorno mental que no le permite tener pleno conocimiento de la conducta, pero claro está que el conocimiento es un elemento característico de un delincuente informático.
- Responsabilidad en embriaguez: Son únicamente en delitos de tránsito.
- Personas menores de dieciocho años: Estas personas serán sometidas acorde al Código Orgánico de la Niñez y adolescencia, bajo la luz de COIP son inimputables, ahora, si un menor de 18 años con una cuenta falsa se llega a crear una cuenta falsa para realizar una estafa.

Cabe recordar que este delito debe tener un beneficio patrimonial, por lo cual el dinero que se haya utilizado debe ser transferido a una cuenta bancaria, de tal modo que, un menor de edad no puede disponer de una, en ese sentido debería utilizar la cuenta de un cómplice, como podría ser su padre de familia donde recaería la responsabilidad por la actuación del menor y se podría interpretar que está manejando la identidad del menor para efectuar el crimen.

Este análisis se realiza en un caso extremo, pero se entiende que un menor de dieciocho años no puede cometer tal delito porque no posee una cuenta bancaria y existiría ausencia de tipicidad al momento en que no se determine una afectación en el patrimonio.

Dentro del mundo informático se han implementado diferentes nombres para los delitos, uno de los más conocidos son el phishing y skimming (Castillo C., 2018).

El phishing es un método que utilizan los ciberdelincuentes para engañar y obtener información persona, generalmente de las tarjetas de crédito y las contraseñas de bancas web, lo realizan a través de e-mails o enlaces fraudulentos que se encuentran dentro de las páginas web, y el skimming es el robo de información de tarjetas de crédito utilizado en el momento de la transacción, con la finalidad de reproducir o clonar la tarjeta de crédito o débito para su posterior uso fraudulento. Consiste en el copiado de la banda magnética de una tarjeta (Castillo C., 2018).

Estos dos términos mencionados están dentro del tipo penal de estafa del artículo 168 inciso 1 y 2, aunque falta que se utilice para obtener beneficio patrimonial, sin embargo, al realizar estos actos tendríamos los dos primeros incisos del artículo 186, por lo que se debe considerar estos métodos como delitos de estafa a través de medios electrónicos.

Es importante resaltar que, en el actual Código Orgánico Integral Penal, el delito de estafa a través de medios electrónicos se encuentra adaptado a las nuevas tecnologías y elaborado con base en la información de los delitos informáticos que han salido a la luz, realizando un cambio completo al enfoque que manejaba el anterior Código Penal, en el cual se lo conocía como apropiación ilícita.

Como hemos podido ver a diferencia del actual COIP, el anterior Código Penal manejaba un concepto directo que engloba los delitos de estafa a través de medios electrónicos, sin embargo, técnicamente no brindaba la antijuricidad, el cual es un elemento para que exista un delito (Padilla, 2015).

El artículo que más se asemeja al anterior código penal es el 190 que es la apropiación fraudulenta por medios electrónicos, pero debemos identificar qué realizaba el anterior Código Penal en su tipificación, teniendo como punto de partida el verbo rector, este sería ‘’utilizar fraudulentamente’’, estableciendo una intencionalidad del sujeto activo al realizar el acto ilícito (Padilla, 2015).

El autor Juan Vizueta en su obra Delitos Informáticos en el Ecuador, en su análisis respecto a este delito, nos dice lo siguiente ‘’(...) los sistemas de información son medios por los cuales datos de importancia son compartidos de modo casi inmediato, entre personas o departamentos, utilizando para ellos diversas formas de comunicación; mientras que, la red electrónica de información es un conjunto de equipos y sistemas de información interconectados electrónicamente.’’

Se puede entender que el objetivo del acto ilícito era la apropiación de los bienes ajenos, lo cual vendría siendo más técnico el actual COIP al implantar como objetivo el beneficio patrimonial, hablando específicamente del delito de estafa a través de medios electrónicos. Cabe recordar que el COIP adecua la conducta a los medios actuales como el phishing y el skimming, siendo estos modelos actuales que están adaptados a la realidad social y a la evolución del internet; contrario al Código Penal que al determinar los medios por los cuales se entenderá que se cometió la falta a dicho artículo establece sistemas de información y redes electrónicas.

Para esto, la misma Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de datos definió los sistemas de información como ‘’…todo dispositivo físico o lógico utilizado para crear, generar, enviar, recibir, procesar, comunicar o almacenar de cualquier forma, mensajes datos’’ y la red electrónica sería la transmisión de información a partir de cualquier sistema electrónico.

De este modo, como se pudo ver reflejado el anterior Código Penal mantenía una adecuación del delito muy general que de todos modos si podía realizar el alcance de los ciberdelitos, a diferencia del COIP que se encuentra establecido de manera más específica para determinar la estafa a través de medios electrónicos, pero el factor común es que ninguno de los dos códigos establece un procedimiento eficaz, diferente y adecuado para identificar el sujeto activo del delito, el cual es extremadamente necesario tal como reflejan las estadísticas, ya que dejan en impunidad a los delincuentes informáticos.

Capítulo III

3. Procedimiento en la investigación del sujeto activo en los delitos de estafa a través de medios electrónicos en el Ecuador

3.1. Proceso de investigación del delito

El inicio del proceso empieza con la denuncia realizada por un ciudadano, ya sea de manera verbal o escrita, la Fiscalía recepta esta información y empieza el proceso de investigación previa en la cual va a tener que determinar elementos de convicción, de cargo y descargo que permitan formular o no una acusación en contra del procesado.

Dicho proceso de investigación tiene un plazo máximo de 90 días, si dentro del plazo no se lograron encontrar elementos de convicción suficientes para formular cargos en contra del procesado, se da por concluido el proceso de investigación.

Cabe destacar que, el ciudadano puede realizar la denuncia por estafa electrónica, sin embargo; si durante el proceso de investigación previa se determina que no representa un delito de estafa electrónica y resulta ser otro tipo penal, Fiscalía solicitará al juez la reformulación de cargos, por lo cual una vez el juez acepte la solicitud, la etapa de la instrucción se ampliará treinta días más improrrogables.

Hay que señalar que del mismo modo se puede estar realizando la investigación previa de un delito que no sea estafa a través de medios electrónicos y resulta que durante la investigación se logra determinar que es el tipo penal antes mencionado, por lo que se mantiene el mismo método de reformulación.

Está claro que los delitos de estafa a través de medios electrónicos presentan un problema al momento de realizar la investigación, debido a que no son personas físicamente determinables, pero durante la investigación el fiscal juntamente con la Unidad de Delitos Informáticos debe agotar todos los recursos suficientes para determinar al presunto delincuente y dar con su domicilio. La estafa al ser un delito que debe tener un perjuicio patrimonial se debe manejar bajo un estricto protocolo de investigación, mismo que se presenta a continuación:

- Solicitud de revisión voluntaria de la información.
- Mandato judicial.

- Orden de registro.

Para realizar la búsqueda del presunto autor del delito, la policía se encargará de la incautación de los equipos electrónicos, indagando los archivos que permitan precisar las actuaciones ilegales, posteriormente se tiene que determinar la información a través de un rastreo y fijación de la IP de las computadoras, en el caso de la alteración de los cajeros automáticos o un medio electrónico que se utilice de manera ilegal para concretar el delito de estafa, se realizarán las encriptaciones de estos aparatos, la desmaterialización de las cámaras de los bancos y todo el rastreo que permita identificar al autor del delito (Díaz & Lascano, 2012).

Dentro de este proceso de investigación, una vez Fiscalía General del Estado recepta la denuncia, pone en conocimiento a la entidad especializada que en los casos de delitos de estafa electrónica es la unidad de delitos informáticos, la cual se encargará del proceso de investigación con el apoyo de criminalística, quien se encargará de la experticia, donde una vez analizado y determinado todos los documentos emitirá el informe técnico a Fiscalía para que continúe con la investigación.

Al momento de lograr determinar al delincuente informático a través de todos los procesos investigativos dentro del plazo de 90 días se realizará la audiencia de formulación de cargos donde se presentarán todos los elementos de convicción recabados por fiscalía y el juez determinará si es procedente para continuar con la audiencia de juicio.

3.2.Tratamiento del delito en Fiscalía

La Fiscalía es la entidad encargada de receptar todas las denuncias de acción penal pública. Una vez ingresada una denuncia, recaban todos los datos necesarios para empezar con la investigación del delito, una vez obtenidos los elementos de convicción suficientes para demostrar que existió un acto ilícito, se realiza la formulación de cargos.

En el caso de los delitos de estafa electrónica, la fiscal María Elena Bayas Santillán en una entrevista realizada, indicó que el tratamiento de las denuncias presentadas por el delito de estafa se realiza igual que cualquier otro delito, a excepción de los crímenes de asesinato y violación que tienen un procedimiento especial en la investigación de la materialidad del delito y presuntos autores.

Fiscalía al recibir una denuncia por estafa electrónica la envía a la unidad especializada que es la Unidad de delitos informáticos, quienes juntamente con la policía cibernética y policía judicial se encargará de realizar toda la investigación pertinente para encontrar al delincuente, todo

este proceso va de la mano con la presunta víctima debido a que se debe contar con toda la información necesaria que soliciten los investigadores para poder llegar a determinar el delito.

Por tal motivo es que existen pocos casos de estafa electrónica con una resolución debido a que no existe la cooperación de los ciudadanos para poder realizar una indagación completa, donde las personas que son víctimas de estafa electrónica son clase media alta, lo que para ellos no es un valor significativo el que deseen reclamar y prefieren solamente denunciar y obtener una mayor seguridad en sus cuentas bancarias.

Dentro del proceso investigativo, la Fiscalía dispone por iniciativa propia o a pedido del denunciante que se practique un peritaje informático para determinar cuáles fueron los móviles desde los cuales se perpetró la estafa por medios electrónicos y las huellas que pudieron haberse generado en los sistemas de datos.

Por lo general, este tipo de peritajes suelen delegarse a peritos informáticos de la policía judicial. En otros casos, el fiscal solicita a la Dirección Nacional de Investigaciones de la Fiscalía que le remita los nombres de una terna de peritos acreditados, para designar a uno de ellos como expertos que analizarán las evidencias informáticas del caso.

Fiscalía formulará cargos cuando existan indicios y anticipos de prueba suficientes para determinar la materialidad del delito de estafa informática, en el cual necesariamente debe existir un resultado cuantificable al patrimonio de la persona natural o jurídica; no obstante, si no se llega a determinar con claridad el nexo causal de los hechos delictivos con un presunto autor, no se podrá pedir la formulación de cargos, porque necesariamente la conducta dañosa que generó resultados en el patrimonio de las víctimas, debe ser atribuible a un sujeto o sujetos en concreto.

La mayoría de los peritajes informáticos encuentra las huellas del delito perpetrado, pero no identifican a los autores reales del delito, sea porque el lugar de la comisión del delito es una computadora de uso público, porque se trata de un computador o terminal que pertenece a otro sujeto distinto del infractor, o bien porque el ciberdelincuente disfraza sus métodos de operación con direcciones falsas, enmascaradas o dinámicas.

Lo dicho anteriormente nos lleva a establecer que pocos casos de estafa electrónica llegan a la etapa de juicio, porque inclusive si se logran determinar presuntos autores de la infracción,

estos sujetos suelen ser agentes intermediarios del delincuente sin rostro que se enmascara en la tecnología para planificar y ejecutar la estafa por medios electrónicos.

Por ende, fiscalía se encarga de todo el proceso investigativo y legal para poder determinar quién es el sujeto activo en los delitos de estafa electrónica, el tratamiento de estos casos está ligado a todo el debido proceso que establece el Código Orgánico Integral Penal, de tal manera que puedan llegar a ser sancionados efectivamente los delitos de estafa informática.

3.3.Tratamiento de la investigación en criminalística

En la entrevista realizada al Ing. Tulio Simba, ex perito de criminalística; expresa que la estafa electrónica es un delito de resultado, en el que criminalística se encarga de realizar la experticia, no la investigación.

Se recibe la solicitud de parte de Fiscalía para realizar el peritaje informático y la determinación técnica de la IP (identificación de red o dispositivo en internet) para analizar el lugar, tiempo, y método del crimen. Dentro de criminalística existe también una unidad especializada para los delitos de estafa electrónica, esta es la Unidad de informática forense, donde se encargan de realizar las diligencias para presentar el informe técnico de los resultados de la indagación.

En el área de informática forense explica cómo se realiza el proceso de nombramiento de peritos, mismo que se da mediante un sorteo, es menester mencionar que la cantidad de peritos que existen para este tipo de delitos es demasiado bajo y escaso. En sus inicios, la unidad en mención contaba con dos peritos especializados en el tema, ahora mismo la unidad cuenta con un número menor a veinte peritos; por ende, resulta difícil encontrar resultados teniendo en cuenta la nueva era digital en la que nos encontramos.

Es importante diferenciar que por parte de la Policía Judicial, la cual trabaja con fiscalía en el proceso de investigación en la Unidad de delitos informáticos, también cuentan con peritos asignados, pero esta tiene fines investigativos, es decir, se encargan de desarrollar la búsqueda del lugar, computador o dispositivo informático que fue utilizado para cometer el delito,

Por parte, los peritos asignados en criminalística realizan el informe técnico partiendo de la IP o los chips que encriptan cuando se utiliza para hackear tarjetas o cuentas bancarias, una vez que el perito de criminalística logra identificar de donde proviene dicha IP o dispositivo

electrónico, elabora un informe pericial y entrega a fiscalía para que este pueda continuar con la investigación.

3.4.Peritaje informático, sus características y utilización como prueba en procesos penales

El peritaje informático se trata de un análisis de una prueba tecnológica que se presenta ante un tribunal de justicia penal, generalmente en los delitos informáticos. A través de este, el perito se encarga de extraer toda la información necesaria de un dispositivo tecnológico, con el fin de obtener un análisis forense, de pruebas, extracción de conclusiones y finalmente presentar el informe sustentado en todo lo investigado (Atico34, 2020).

El peritaje informático consta de 4 premisas dentro de un proceso judicial:

1. Conseguir toda la información y documentación necesaria para esclarecer el consumado.
2. Cimentación del relato fáctico.
3. El informe debe ser fundamentado en razonamientos lógicos a partir de toda la información extraída en el estudio forense que se realizó, además que debe estar redactado y explicado en un lenguaje entendible para el juez, el cual no es especialista en esta área.
4. El informe pericial debe ser explicado por el perito de manera oral, donde sustente las conclusiones a las cuales ha llegado (Rodríguez, 2022).

Su valor probatorio es fundamental, ya que permite tener una base y una conexión específica al medio al que se encuentra ligado para poder dar con el sujeto activo del delito. Sin embargo, la evidencia digital es anónima, duplicable, alterable y eliminable, por ellos se entiende que existe una división para fundamentar una evidencia digital (Sampaoli, 2018).

Primero, se presentan los registros almacenados en un equipo informático como chips, correos; segundo, se demuestran los registros generados por un equipo informático los cuales puedes ser logs de errores o logs de transacciones; finalmente, uno de los más importantes que es los registros parcialmente generados y almacenados en un equipo informático, los cuales pueden ser códigos o escaneos momentáneos, siendo archivos que se generan temporalmente en internet (Sampaoli, 2018).

En conclusión, el peritaje informático en los delitos de estafa electrónica, teniendo en cuenta que este delito tiene que tener una afectación patrimonial, en el momento de la prueba debe analizarse las evidencias que se relacionen con agendas virtuales, agenda con direcciones, información de las

tarjetas bancarias, información de las cuentas bancaria y finalmente de los clientes, esto con el fin de enlazar los sujetos que estén involucrados dentro de estos delitos, ya que al tomar dinero de una cuenta, obligatoriamente debe existir la conexión en otra entidad bancaria o financiera (Sampaoli, 2018).

3.5.Ineficacia en el procedimiento de identificación del sujeto activo

3.5.1. Vacío legal

El artículo 186 del Código Orgánico Integral Penal, regula la estafa electrónica, siendo este el único artículo que hace referencia al tipo penal, por lo que resulta muy amplio y ambiguo si este no se complementa con un proceso adecuado a la identificación del sujeto activo del delito, permitiendo así que los delincuentes que realicen estafa a través de medios digitales queden en impunidad, además de que la gente desista de continuar con el procedimiento.

Por otra parte, generalmente la investigación de este tipo de delito se estanca hasta la denuncia presentada por los afectados, ya que terminan desistiendo del proceso o como se mencionó anteriormente, no se encuentran los elementos de convicción suficientes que adecuen la conducta al tipo penal, de tal modo se evidencia que no existe una normativa con un procedimiento de investigación adecuado, ni un método para prevenir y combatir eficazmente a los delincuentes informáticos, poniendo en peligro el patrimonio de los ciudadanos y causando un perjuicio irreversible.

Es importante resaltar que los bancos juegan un papel relevante dentro de la protección digital a las cuentas bancarias, donde existe un vacío normativo que favorece a los bancos y los mantiene blindados para eximirse de responsabilidad, siendo este un error grave que debe ser atendido inmediatamente, puesto que los bancos no invierten en seguridad para sus clientes, por ende el Estado debe procurar incorporar normas que obliguen a las entidades bancarias a mejorar su política de seguridad antes e incluso después del delito.

3.5.2. Recursos prácticos

Primero hay que empezar por entender que la capacidad tecnológica con la que cuenta el Estado ecuatoriano está en proceso de desarrollo, no se encuentra con una base consolidada como en Europa.

Cabe determinar recursos prácticos puntuales que perjudican a la identificación del sujeto activo en los delitos de estafa electrónica, los cuales son: la velocidad de internet con la que cuenta Ecuador, en el 2020 el portal Ookla en su informe Speedtest Global Index el cual hace un análisis de la velocidad de internet de cada país, logró determinar que Ecuador se encuentra por debajo de los promedios de una velocidad de internet normal, es decir su velocidad de internet es demasiada baja (Dávalos, 2020).

Por otra parte, tal como manifestó el Ingeniero Tulio Simba, de la Unidad de informática forense, en la entrevista que realicé, la cantidad de peritos especializados que existen en esta área es escaso para la era en la que nos encontramos, básicamente, es imposible lograr controlar la estafa electrónica y mucho menos llegar a determinar quiénes pueden ser los autores de estos delitos si no se cuenta con un personal suficiente que pueda elaborar una correcta laboral dentro de los peritajes e investigación.

Es menester mencionar que, no existe una campaña de concientización que permita a los ciudadanos tener conocimientos básicos en ciberseguridad, especialmente en sus tarjetas o cuentas de banco para que no puedan ser víctimas de este delito, no existe un método de prevención adecuado a la realidad tecnológica en la que nos encontramos. Además, el Estado ecuatoriano no ha utilizado medidas de prevención informáticas a la ciudadanía, que permitan advertir que los delincuentes informáticos son igual de peligrosos que los que comúnmente se conoce, existe un desconocimiento por parte de la sociedad respecto de la situación criminal tecnológica.

Por ende, no se ha visto una manifestación por parte de la sociedad para que el Estado ejerza los suficientes recursos prácticos preventivos para evitar la estafa electrónica, y por parte de los legisladores, no se ha establecido un protocolo eficiente para poder identificar a los sujetos activos de este delito, teniendo en cuenta que el termómetro social en el que no encontramos es la era digital, por lo que el derecho debe de ir evolucionando de la mano con los nuevos retos que enfrentan los ciudadanos.

Capítulo IV

4. Análisis de jurisprudencia sobre delitos de estafa y apropiación ilícita por medios informáticos y electrónicos

En el Ecuador existen pocos casos con sentencia ejecutoriada respecto al delito de estafa a través de medios electrónicos, como hemos analizado existen un antes y un después con el ingreso del COIP, ya que, en el Código Penal, la cual era la normativa vigente anterior al COIP, este delito se conocía como apropiación ilícita.

En la actual normativa contamos igualmente con la tipificación de la apropiación ilícita, pero se ha aumentado en el artículo 186 numeral 1 y 2 la especificación de la estafa por método informáticos en las cuentas bancarias, por ello, vamos a realizar un análisis jurisprudencial mediante el cual va a permitir esclarecer cómo el sistema de justicia ha realizado las investigaciones para identificar al sujeto activo en este delito.

4.1.Proceso No. 17294-2020-00949

En el proceso N.- 17294-2020-00949 contamos con una estafa a través de medios electrónicos, la infracción por la cual se inicia el proceso es la vulneración del artículo 186 numeral 1, claro está que no existe una sentencia ejecutoriada, pero si se llegó a cumplir con la etapa de investigación previa para la formulación de cargos, cabe resaltar que los cargos no fueron formulados porque fiscalía decidió desistir del proceso, sin embargo, si se cuenta con todos los elementos de convicción recabados que se iban a utilizar para formular cargos. Es importante entender esto porque en la denuncia No.170101816085620 no se reconoce al sospechoso, y posteriormente se logra identificar.

En este caso tenemos como víctima a la empresa ‘’PLASTIAZUAY’’, la cual es una empresa que se dedica a la venta de varios productos, siendo principalmente la cuerina.

Los primeros días de junio del 2016 la empresa DIMELROV, INGENIERÍA Y SERVICIOS por medio del señor Andrés R. el cual indicó ser representante legal de esta compañía tomó contacto con la empresa víctima para consultar respecto a ciertos materiales, después de varios días de consultas finalmente decidió realizar una compra a través de una dirección de correo electrónico ficticio, el cual supuestamente era un correo de la compañía, DIMELROV se

encontraba ubicada en Quito, pero el señor había solicitado dentro de su compra que el material sea entregado en Latacunga y que enviaría a otra persona que recoja el pedido.

Una vez que el pedido fue entregado en el punto solicitado, procedieron a pagar con dos cheques los cuales cubrían el valor total de los pedidos, sin embargo, 3 días después fueron devueltos estos cheques, por el banco debido a insuficiencia de fondos y anulación. Al momento en que quisieron contactar al señor a través del correo electrónico no lo encontraron, al buscar a la empresa pudieron contactar a un socio el cual les supo manifestar que le habían sustraído la chequera, pero les brindó la ubicación del señor Andrés R.

Finalmente, después de todo lo mencionado se realizó la denuncia para que se siga todo el proceso legal y se devuelva el dinero a la empresa PLASTIAZUAY.

En lo que respecta al caso, es importante analizar que la estafa se realiza a través de un medio electrónico, en este caso un correo electrónico donde el mismo fue utilizado como notificación del pago. El proceso de investigación que se realizó fue primero identificar quien es la persona que realizó las consultas, porque la compra fue realizada por un correo electrónico falso, es decir, una identidad electrónica alterada, la cual no permite identificar a un sujeto físico. Por lo consiguiente, para poder identificar al sujeto activo de este delito, fiscalía solicitó las siguientes diligencias:

1) Que se oficie al jefe de Coordinación de la Fiscalía de la Policía Judicial de Pichincha, a fin de que delegue un agente a su cargo, el mismo que deberá encargarse de reconocer los lugares, huellas, señales, armas, objetos e instrumentos con la intervención del personal del Sistema especializado integral de investigación, medicina legal y ciencias forenses
2) Disponer al personal del Sistema Especializado Integral de Investigación, médica legal y ciencias forenses la práctica de diligencias tendientes al esclarecimiento del hecho, salvo la recepción de la versión del sospechoso.
3) Recibir las versiones de la víctima y de las personas que presenciaron los hechos o de aquellas a quienes les conste algún dato sobre el hecho o sus autores
4) El agente investigador designado debía presentar el respectivo informe en un plazo de 30 días una vez entregado el oficio de las diligencias.
5) Finalmente, a la víctima se llamó a que diera su versión libre y voluntaria respecto a los hechos.

Una vez que fueron realizadas todas estas diligencias, se determinó que los autores implicados de este delito eran el señor Andrés R. (por motivos de seguridad no se redactan sus nombres y apellidos) y Paúl F. quien es la persona a quien fue entregado el pedido y realizó el pago de los cheques. Pero, la investigación no fue concluida debido a que debe existir una certeza en la identificación del sujeto activo, por ello la fiscal encargada del caso requiere información adicional, la cual es:

1) Receptar la versión libre y voluntaria sin juramento del señor Andrés R.
2) Un oficio al SRI donde conste los datos actualizados de la empresa DIMELROV.
3) Oficiar a la Jefatura Provincial de Criminalística de Pichincha, para la designación de peritos para la realización de una pericia grafológica de las firmas impuestas en los cheques.
4) Que se oficie a la Policía Judicial de Pichincha, para la designación de un agente investigador de la unidad de Delitos Informáticos, a fin de que determine el punto IP y el titular del correo electrónico de PLASTIAZUAY y de DIMELROV.
5) Un oficio a la Policía Judicial de Pichincha, donde designe un agente investigador que remita un álbum fotográfico de Andrés R. y Paúl F., a fin de realizar la diligencia de reconocimiento fotográfico.

De acuerdo con las diligencias que fueron realizadas dentro de la Investigación Previa No. 170101816085620, la fiscal solicita al juez que se realice la formulación de cargos, ya que han encontrado los elementos de convicción suficientes donde posiblemente existe tal hecho ilícito y se ha podido identificar a los presuntos autores del delito.

De este modo, se ha realizado una investigación muy completa, aunque el caso no cuenta con una sentencia ejecutoriada, se puede evidenciar que se necesita un trabajo informático para determinar el lugar y los autores de la escena del crimen, también es importante resaltar que se debe demostrar que existió un engaño, induciendo a un error, pero causando el perjuicio y desplazamiento patrimonial.

En lo que respecta a la identificación de los sospechosos, es relevante además de encontrar físicamente a los autores, también realizar las diligencias que permitan asegurarse de que ellos son los que participaron dentro de estos actos, porque caso contrario se perjudica a un proceso y a las personas que no tienen nada que ver dentro del mismo. Por ende, se cuenta con recursos suficientes

para lograr determinar los autores del delito, pero también existe una colaboración constante de las víctimas lo cual facilita todo el proceso.

Ahora, en comparación con el sistema de justicia europeo, donde la identificación y juzgamiento de delitos informáticos se encuentra mucho más avanzado que en el sistema de justicia ecuatoriano.

El Tribunal Supremo de la Sala Segunda de lo Penal de España, resuelve un recurso contra una sentencia de Audiencia Provisional de Madrid, donde se declara culpable a una persona de cometer un delito de estafa electrónica, por lo cual en casación se realiza un análisis completo adecuado a una ardua y técnica investigación para poder entender por qué se ha determinado autora del delito de estafa electrónica.

4.2.Sentencia No. 509/2018. España, Madrid

El caso trata de una señora (en adelante se le mencionará acusada) que acompañaba a realizar pagos a un señor, el cual era mayor de edad (en adelante se le llamará víctima) en el cual su relación era cercana, ya que la acusada era novia de un sobrino de la víctima, quien al ser una presunta persona de confianza le encargaron a que le acompañe a realizar gestiones bancarías, ya que el señor era un adulto mayor, quien apenas podía leer y escribir, pero no tenía conocimiento alguno de cómo manejar las cartillas del banco.

Ante esto, la acusada se aprovecha de la situación para poder tomar el número secreto de la cartilla de la víctima, que en palabras más sencillas es la clave para poder retirar el dinero en los cajeros automáticos o realizar transacciones, y efectúa varios reintegros en la cartilla, siendo uno de ellos el 1 de junio de 2015 una transferencia de 3.000 euros desde la cuenta bancaria de la víctima hacia la cuenta de la acusada, apoderándose en total, de 16.520 euros.

Ante esto, podremos ver todos los argumentos de derecho que utilizó esta sala para llegar a la determinación del delito. Primero, el tribunal desglosa la estafa informática, es decir, parte de un análisis que permita identificar si incurre en este delito.

El hecho fundamental de la estafa es que debe existir engaño, por tal se podría entender que la acusada no realiza ninguna engaño a la víctima, únicamente toma posesión de las cuentas aprovechando de la situación del adulto mayor y a partir de ello realiza el desplazamiento del dinero a su cuenta bancaria, de hecho en los escritos de acusación formulados por el Ministerio

Fiscal, en la querella, y en la primera sentencia no se especifica un engaño, ya que la desposesión del bien ajeno como se mencionó anteriormente se lo realiza por medio de una apropiación indebida.

Respecto a dicha sentencia, el tribunal supremo no concuerda con la argumentación de los jueces, recalcando que existe una falta de motivación y análisis en la misma. Por ello, al recoger todas las pruebas documentales y testimoniales donde se incluye al trabajador del banco donde fue sustraído el dinero, argumentan que en las instancias anteriores obviaron el hecho de que para retirar el dinero de los cajeros automáticos es necesario una clave de acceso, un código o un pin, que la acusada consigue aprovechando de la situación de la víctima.

A partir de esto, se entiende que hablamos de una estafa y no de un hurto, porque al momento en que se realiza la operación para ‘’recibir’’ el dinero y no ‘’tomarlo’’, la persona recae en esta acción al ser el banco o el cajero automático quien le entrega este dinero, es decir, es dado por una máquina más no por la persona titular de la cuenta.

Como segundo punto en los fundamentos del tribunal, se utiliza la misma línea de argumentación tomada de la sentencia No. 369/2007 y en el artículo 248.2º literal a) del Código Penal de España, donde se menciona:

> *(...) También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de otro’’.*

La apreciación de estafa a resultado difícil por problemas de identificación del tipo penal, y se ha estudiado de manera doctrinal que un engaño no puede ser realizado a una máquina, sino a una persona, y este cajero al ser programado teniendo una funcionalidad mecánica, pues la acción de programación fue realizada por una persona, dando así una ecuación que el engaño surge contra la persona que programó el artefacto electrónico.

De tal manera, al sustraer la persona una tarjeta o pin de acceso para la cuenta bancaria, y utilizarla para retirar el dinero, emitiendo la orden al cajero, logra demostrar una identificación fraudulenta del cajero, simulando ser el titular de la cuenta y de esta manera estamos hablando de que el engaño no surge contra el dueño de la cuenta, ni mucho menos al cajero automático, por el contrario, el tribunal precisa que el acto de engaño fue realizado al banco.

Estamos hablando de un acto ilícito en contra de una persona jurídica, logrando obtener ilegalmente un desplazamiento patrimonial ocasionado por un error involuntario, es decir, induce a error al banco o al trabajador de este, concluyendo que ha logrado engañar induciendo a error al banco y obteniendo un beneficio patrimonial perjudicando al dueño de la cuenta.

Es importante, en este punto, entender que no se puede asimilar que el cajero automático es el fin de este medio, es decir, que la máquina es quien entrega el dinero, sino que este es parte de un proceso informático y sirve de un medio del banco, siendo la institución bancaria quien a través de una voluntad viciada con la confianza errónea de operar con el titular de la cuenta que realiza la transacción de este patrimonio.

A los ojos de la ley, es imposible que una máquina sea engañada, debido a que solamente está actuando de forma programada, y el engaño solo recae cuando es de una persona a otra a través de una interacción. Por tal, se recurre a lo práctico y no a guiarse en el sentido literal de la norma.

Ante esto, se procede a interpretar que al digitar el código dentro de un cajero o una cuenta bancaria básicamente es la manera de identificarse dentro del mismo, y al utilizar claves o códigos que hagan entender al cajero automático que se está tratando con el titular de la cuenta, pero no resulta ser verdad, se estaría incurriendo en una manipulación informática, que es la que permite determinar que estamos frente a una estafa a través de medios electrónicos.

Los pronunciamientos contenidos en el tercer y cuarto punto mantienen su fundamento en jurisprudencia de España, en casos que guardan similitud y su análisis determina una misma conclusión, el engaño no puede ser exigido, donde se debe respetar la narración de los hechos, debido a que el concepto de ‘’engaño’’ e ‘’inducir a error’’ es muy amplio, pero tampoco inentendible.

Se procedió a analizar los hechos acontecidos y acompañarlos de una correcta apreciación y adecuación a la norma, aclarando que el elemento normativo que permitir realizar una correcta apreciación del caso es la obtención y ejecución de la clave de acceso, recayendo similarmente a una manipulación informática, pero que dé a partir de ello, han podido determinar y concluir que el delito es una estafa electrónica.

Como último punto y dictamen final se aclara que no se realiza un análisis subjetivo a partir de las versiones, el punto de interpretativo es netamente jurídico, realiza una mezcla jurisprudencial y normativa.

El fallo del Tribunal de Justicia es el siguiente:

> ‘’(…) indica cómo eran las relaciones previas al momento contemplado en autos cuando ya actúa para conseguir el PIN; lo que conlleva por interacción de los art 74 CP y 249 CP que la pena a imponer haya de encontrarse entre el año y nueve meses y los tres años de prisión; y al umbral mínimo habremos de estar, al ponderarse el artificio y la reiteración de actuaciones en la calificación efectuada y no contar con datos significativos sobre la personalidad de la acusada; y en cuanto a la responsabilidad civil habrá de estarse a los 16,520 euros obtenidos, sin consideración alguna a los daños morales al no haber sido declarada su existencia en el relato probado de la sentencia de instancia’’.

Como hemos podido analizar, el tribunal efectuó un estudio completo, donde acusan a la señora de criminalmente ser responsable del delito de estafa informática, pero realiza una correcta distinción entre hurto, apropiación indebida y estafa, siendo importante mantener una normativa que garantice la seguridad jurídica a los ciudadanos.

4.3. Proceso No. 17123-2012-0240

El presente caso es juzgado bajo el anterior Código Penal, condenando al señor Giovanny como autor del delito de apropiación ilícita. Este juicio es seguido por el Banco Pichincha, quien es el perjudicado en este caso.

Primero, se presentan los hechos del caso; donde Giovanny era Gerente General de la compañía ‘’Espend’’, la cual tenía un convenio con el Banco Pichincha, el 28 de enero del 2008 el señor Giovanny deja de ser gerente de esta empresa, posteriormente al haber concluido sus funciones el autor del delito se realiza una transferencia de dinero proveniente del patrimonio de la empresa ‘’Espend’’ utilizando como medio al banco pichincha, esta fue realizada hacia su cuenta personal, cuyo monto fue un total de $21.200.00 dólares americanos con fecha 18 y 19 de abril del 2008.

Es importante destacar que Giovanny cuando era gerente de la empresa, en el sistema de CASH MANAGEMENT contaba con perfil full el cual le permitía aprobar las transacciones de transferencia/pagos electrónicos de la Empresa ESPEND.

Ante todos los hechos mencionados, el procurador judicial del Banco Pichincha realiza la denuncia por apropiación ilícita, dónde la fiscalía para el proceso de investigación utiliza dos peritos, quienes cuentan con conocimiento especializado en experticia informática y uno de ellos ha realizado más de cien peritajes informáticos.

El fin de la investigación pericial fue para determinar que el perfil FULL permite realizar todas las transferencias sin ningún permiso, ya que, a partir de este usuario, se tiene el control del dinero que se encuentra de manera electrónica, de este modo realizando la determinación de quien manejaba tal perfil, a raíz de las claves únicas que permitían acceder al mismo, más no de una encriptación de la IP, y, por otro lado, la determinación del propietario de las cuentas en las cuales fueron recibidas estas transacciones.

De tal modo, que a través de esta conexión de los hechos se da con la persona de manera física, y se pone a las órdenes de la justicia, donde se dictamina sentencia, acusándolo de ser responsable por el delito de apropiación ilícita.

Actualmente, con la reforma del COIP este caso no sería juzgado por apropiación ilícita, porque no encajaría con el tipo penal, entendiendo que la estafa a través de medios electrónicos es un delito de resultado que debe cumplir con 4 factores para que entender que se adecua a este tipo penal y estos son la acción de engaño, que induzca a error, el cual cause un perjuicio patrimonial y el desplazamiento de este donde finalmente tiene que ser causado este perjuicio por un medio informático o electrónico.

Por ello, en este caso encontramos la identidad del autor del delito en el internet, donde claramente es mucho más fácil identificarlo porque se maneja a través de un usuario y contraseña único asignado a una persona.

En los alegatos de los recursos de apelación y nulidad, Giovanny alega que existieron omisiones importantes en la investigación, una de ellas es la determinación de la IP a través de la cual fue realizado el ingreso a la plataforma para transferirse el dinero y la falta de esta ocasiona que no se realice una investigación transparente afectando al debido proceso.

Ante esta situación, los jueces concuerdan que no es necesario la determinación de la IP, ya que, la identidad física es determinable a partir de que él es la única persona que manejaba tal usuario y que en el caso de que otra persona ingrese con este perfil no utilizaría la cuenta de un tercero para transferirse el dinero, por ende, basta con la identidad del perfil desde donde se realizó la transferencia y la cuenta donde llegó este dinero para poder determinar quién es el sujeto activo de este delito.

Una vez identificado el autor del delito, podemos ver que a partir del perfil full con el que contaba lo utiliza para engañar al Banco Pichincha, porque él está realizando dicha acción fuera de sus competencias, teniendo en cuenta que ya no era gerente de la empresa, de este modo se aprovechó para insinuar al banco que está tratando con un gerente actual, de tal manera que juntamente con esta acción de engaño, insinúa a error ocasionando que el dinero sea transferido a la cuenta de Giovanny.

Por este motivo es fundamental la postura de los jueces al no dar importancia a la determinación IP, primero por no sacrificar la justicia solamente por la omisión de procesos y segundo porque se tiene plenamente identificado al beneficiario del dinero que coincide con el propietario del usuario que realizó la misma, que en otras palabras tal como lo menciona el perito ‘’la transferencia genera orden y transmite fondos, el funcionario que tiene la clave es el que ordenó la transacción era la persona que tiene la clave, identidad informática que es lo que se llama actualmente.’’

Un punto importante es ver reflejado que se cuenta con peritos con más de cien experticias informáticas lo cual es un punto a favor dentro del procedimiento de investigación, sin embargo, dentro de las declaraciones en el caso, el perito menciona que no se puede determinar la IP, a pesar de que no sea relevante dentro de la investigación, es preocupante el hecho de no lograr realizar dicho proceso teniendo en cuenta que este caso no cuenta con una complejidad informática, pero en otros casos en los que se requiera dicha información pone en peligro la justicia dentro de estos delitos.

Por otro lado, el punto a destacar es la comparación de la tipificación del delito de apropiación ilícita realizada en el Código Penal en comparación con el Código Orgánico Integral Penal que es el código vigente.

El banco en su testimonio y su denuncia dice lo siguiente *''realizamos la denuncia por apropiación ilícita por utilizar sistema informático de manera fraudulenta''*, pero como hemos podido analizar acorde al análisis de los jueces, no estamos tratando una apropiación ilícita y mucho menos ningún otro delito, debido a que el señor Giovanny está utilizando una identidad falsa que ya no le pertenecía, de tal modo que adecuándose a la normativa actual que es el COIP, a pesar de que no se encuentra bien adecuado al tipo penal estaríamos hablando de una estafa a través de medios electrónicos.

Finalmente, la relación de causalidad entre la acción y el resultado de la actuación producida por el sujeto activo consiste en la materialidad del tipo tal como se ha pronunciado fiscalía, verificando de este modo que, al ser un delito de resultado, es un delito doloso, es decir, el verbo rector que acorde al Código Penal fue adecuado este delito, encaja en la conducta de apropiación ilícita con el resultado del pensamiento, conocimiento y voluntad, donde el autor domina el hecho.

CONCLUSIONES

1.- La cantidad de delitos por estafa a través de medios electrónicos que suceden día a día en el Ecuador, es muy alta, y, representa un peligro cada vez más elevado para el patrimonio de los ciudadanos ecuatorianos, debido a que el mundo actualmente se encuentra en una constante evolución digital, por ende, los ciberdelincuentes cuentan con plataformas y medios digitales cada vez más avanzados, mientras que, los niveles de protección informática de las personas naturales y jurídicas en el Ecuador disminuyen.

2.- El problema de la ciberdelincuencia lo ha enfrentado el mundo entero, sin embargo, como hemos podido analizar, el Ecuador no cuenta con una normativa completamente adecuada y perfilada respecto de los delitos de estafa cometidos por medios informáticos y electrónicos, normativa eficaz que permita brindar seguridad a los ciudadanos. La situación actual deja en evidencia, la inseguridad jurídica que tiene nuestro país, al no poseer un proceso eficaz ni una respuesta oportuna para poder identificar a los sujetos activos de estos ilícitos, con el fin de sancionarlos y de resarcir el daño causado a las víctimas en su patrimonio y actividades.

3.- En el sistema penal del Ecuador se estableció una primera tipificación de actos similares a los de la actual estafa electrónica, los cuales se hallaban bajo la figura de la apropiación ilícita por medios informáticos o electrónicos, en el Código Penal anterior a la vigencia del actual COIP.

Esta tipificación que hacía el anterior Código Penal de la apropiación ilícita, si se compara con ejemplos de las legislaciones europeas y sus resoluciones, no guardaba ninguna relación con la estafa a través de medios informáticos, donde si bien, ambos delitos son de resultado, las características de cada tipo son distintas, principalmente la estafa electrónica solo concurre si existe engaño, error, desplazamiento patrimonial y perjuicio.

El engaño es el elemento más significativo del delito de estafa, porque es el presupuesto fundamental para determinar la relación de causalidad, de tal manera que, el engaño es el motivo o la causa del perjuicio patrimonial y es el elemento diferencial no solamente frente a la apropiación ilícita, sino también frente a otros delitos contra el patrimonio como son el hurto o el abuso de confianza.

4.- El COIP incorporó como modalidades de la estafa electrónica, a los hackeos y clonaciones de tarjetas y contraseñas de los usuarios clientes de los bancos, pero el enfoque va

realizado más al defraude, lo que deja en evidencia que existe una laguna normativa que no permite realizar un correcto proceso al momento de identificar el delito y al sujeto activo del mismo.

De igual manera, la cantidad de técnicos y peritos especializados en el área de delitos informáticos en el Ecuador es escasa, por lo cual, al no contar con los recursos prácticos suficientes para enfrentar este delito y acompañado de una inseguridad normativa, dan como resultado una alta tasa de impunidad en la mayoría de los casos.

A través de la investigación de campo y visita a la Fiscalía con entrevista, se ha constatado que en la mayoría de los casos, los afectados por el delito de estafa por medios informáticos o electrónicos, llegan solamente a presentar una denuncia en fiscalía y en muy pocos casos, avanza la indagación previa y las fases procesales.

5.- Considerando que, autores y tratadistas del derecho han identificado a los delincuentes cibernéticos como criminales temidos por la sociedad, el estado no ha planteado una solución a este problema, debido a que, no se han utilizado adecuadas medidas preventivas que permitan alertar a la ciudadanía respecto a este tipo de delincuentes y el peligro real que representan dentro de la sociedad, y si bien, los recursos prácticos son vitales para fortalecer el proceso de identificación, la implementación de una normativa técnica es fundamental para que la imputación objetiva de la conducta esté adecuada al alcance de la norma.

6.- Es importante mencionar que, la investigación para identificar al sujeto activo en el delito de estafa electrónica es bastante compleja, teniendo en cuenta que la persona físicamente no es identificada, su identidad es a través de internet, y a está, ser alterable se necesita de recursos elevados e idóneos para poder realizar una correcta investigación, pero, tal como mencionaron los servidores públicos profesionales que colaboraron con esta investigación, es de suma importancia contar con la colaboración de los ciudadanos para poder identificar a los delincuentes de manera física con el fin de llevarlos ante la justicia.

7.- Como resultado de esta investigación, se ha podido identificar que, el sistema de justicia penal ecuatoriano no cuenta con una normativa que permita identificar eficazmente a los autores de la estafa electrónica, acompañado del hecho de que los recursos prácticos, tales como sistema de internet, peritos y policías especializados en ciberdelitos, son poco preparados y escasos.

Esta situación ha conllevado a que el proceso penal para perseguir estos delitos en el Ecuador, quede únicamente hasta la denuncia, situación que se agrava en virtud de que el estado ecuatoriano no ha tomado medidas importantes para impulsar de una manera eficaz, que los bancos refuercen su seguridad y tampoco ha contado con medidas preventivas que ayuden a la ciudadanía a prever de la mejor manera estos delitos, perjudicando de una manera cada vez más creciente, el patrimonio de los ciudadanos, y, permitiendo la impunidad de los autores "sin rostro" de este tipo de estafas, por un ineficaz proceso de identificación de estos responsables penales, lo que impide su procesamiento penal.

BIBLIOGRAFÍA

Americanos, O. d. (2018). Organización de los Estados Americanos. Retrieved from Organización de los Estados Americanos: https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

Atico34, G. (2020, mayo 26). Grupo Atico34. Retrieved from Grupo Atico34: https://protecciondatos-lopd.com/empresas/perito-informatico-peritaje/

Castillo, C. (2018, noviembre 29). BBVA. Retrieved from BBVA: https://www.bbva.com/es/phishing-vishing-smishing-que-son-y-como-protegerse-de-estas-amenazas/

Castillo, R. B. (2018, junio). Fundación Internacional de Ciencias Penales. Retrieved from Fundación Internacional de Ciencias Penales: https://ficp.es/wp-content/uploads/2019/03/Barrado-Castillo.-Comunicaci%C3%B3n.pdf

Cruz, C. A. (2016, diciembre). Repositorio Digital de la Universidad Nacional de Loja. Retrieved from Repositorio Digital de la Universidad Nacional de Loja: https://dspace.unl.edu.ec/jspui/bitstream/123456789/17916/1/Tesis%20Lista%20Carolin.pdf

Dávalos, N. (2020, julio 18). Primiciasec. Retrieved from Primiciasec: https://www.primicias.ec/noticias/tecnologia/velocidad-internet-ecuador-debajo-promedio-global/

Díaz, A. d., & Lascano, C. M. (2012, julio). Repositorio Institucional Universidad Politécnica Salesiana. Retrieved from Repositorio Institucional Universidad Politécnica Salesiana: https://dspace.ups.edu.ec/bitstream/123456789/2812/1/UPS-GT000312.pdf

Francisco, R. J. (2012). Los Delitos Informáticos y su tipificación en la Legislación Ecuatoriana. Loja: Universidad Nacional de Loja.

Gamón, V. P. (2017, junio 29). Revista Latinoamericana de Estudios de Seguridad. Retrieved from Revista Latinoamericana de Estudios de Seguridad: http://dx.doi.org/10.17141/urvio.20.2017.2563

HOYOS, G. B. (2011). EL DELITO DE ESTAFA INFORMÁTICA EN EL DERECHO EUROPEO CONTINENTAL. Chile: Revista de Derecho y Ciencias Penales Nº 17 (111-149).

J., G., Bermeo, J., Villacreses, E., & Guerrero, J. (2018). DELITOS INFORMÁTICOS: UNA REVISIÓN EN LATINOAMÉRICA. Machala: Centro de Investigaciones UTMACH.

Lara, M. &. (2014, mayo). Hacia una regulación de los delitos informáticos. Chile: REVISTA CHILENA DE DERECHO Y TECNOLOGÍA. Retrieved from Universidad Técnica de Machala: file:///C:/Users/pc/Downloads/262-Texto%20del%20art%C3%ADculo-401-1-10-20180716%20(3).pdf

Liliana, P. V. (2020). "LAS NUEVAS PERSPECTIVAS REGULATORIAS DE DELITOS". Riobamba: Universidad Nacional de Chimborazo.

López, S. L. (2014, enero 1). Informática Jurídica. Retrieved from Informática Jurídica: https://www.informatica-juridica.com/trabajos/posibles-sujetos-de-los-delitos-informaticos/

Padilla, M. P. (2015). La responsabilidad bancaria frente a los delitos informáticos. Quito: Repositorio Institucional UASB-DIGITAL con licencia Creative Commons 3.0 Ecuador.

Padilla, M. P. (2015). La responsabilidad bancaria frente a los delitos informáticos. Quito: Repositorio Institucional UASB-DIGITAL con licencia Creative Commons 3.0 Ecuador.

ROBLEDO, E. P.-L. (LA NUEVA NORMATIVA EUROPEA PARA LA PROTECCIÓN DE LOS DATOS PERSONALES). LA NUEVA NORMATIVA EUROPEA PARA LA PROTECCIÓN DE LOS DATOS PERSONALES. ("LA NUEVA NORMATIVA EUROPEA PARA LA PROTECCIÓN DE LOS DATOS ... - Dykinson") Madrid: Universidad de Sevilla.

Rodríguez, P. D. (2022). Indalics Peritajes Informáticos. Retrieved from Indalics Peritajes Informáticos: https://indalics.com/blog-peritaje-informatico/perito-informatico-peritaje

Sampaoli, J. A. (2018, diciembre 06). Biblioteca Digital de la Universidad Católica Argentina. Retrieved from Biblioteca Digital de la Universidad Católica Argentina: https://repositorio.uca.edu.ar/bitstream/123456789/523/11/peritaje-marco-tecnico-practico.pdf

Caso de apropiación ilícita No. 17123-2012-0240. (12 de septiembre del 2012). Consulta de Procesos del Consejo de la Judicatura.

Caso de estafa electrónica. Sentencia No. 509/2018. (26 de octubre de 2018). España, Madrid. https://vlex.es/vid/745475057

Caso de estafa electrónica. Proceso No. 17294-2020-00949. (05 de septiembre del 2016). Expediente fiscal No. 170101816085620.