PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

ESCUELA CIENCIAS SOCIALES Y HUMANIDADES

TRABAJO DE INTEGRACIÓN CURRICULAR/TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADO (A)

TEMA

LA APROPIACIÓN FRAUDULENTA POR MEDIOS ELECTRÓNICOS: ANÁLISIS DEL TIPO PENAL EN EL COIP

ANDERSON MAURICIO HERNÁNDEZ ARÉVALO

JOSÉ ALEJANDRO NARVÁEZ TACURI

TUTOR: DR. JAIME ALVEAR

IBARRA – ECUADOR

AGOSTO, 2025

Ibarra, 03 de marzo del 2026

CERTIFICACIÓN TUTOR

En mi calidad de Tutor del Trabajo de titulación titulado: LA APROPIACIÓN FRAUDULENTA POR MEDIOS ELECTRÓNICOS: ANÁLISIS DEL TIPO PENAL EN EL COIP, presentado por los estudiantes ANDERSON MAURICIO HERNÁNDEZ ARÉVALO y JOSÉ ALEJANDRO NARVÁEZ TACURI con cédulas de ciudadanía N° 100398994-2 y 100444299-0, para obtener el Título de Abogado.

Certifico que el trabajo cumple con todos los parámetros establecidos, mediante el cual el estudiante demuestra el desarrollo de competencias en el campo de conocimiento de su profesión con un nivel de argumentación coherente, para ser sometido a la evaluación por parte de los lectores.

Adicionalmente, se adjunta el certificado de porcentaje de originalidad de TURNITIN.


LA APROPIACION FRAUDULENTA POR MEDIOS ELECTRÓNICOS: ANÁLISIS DEL TIPO PENAL EN EL COIP

INFORME DE ORIGINALIDAD

7%	7%	4%	6%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	biblioteca.defensoria.gob.ec Fuente de Internet	1%
2	Submitted to Universidad Tecnológica Indoamerica Trabajo del estudiante	1%
3	www.informatica-juridica.com Fuente de Internet	1%
4	Submitted to Universidad Catolica De Cuenca Trabajo del estudiante	<1%
5	Submitted to UNIV DE LAS AMERICAS Trabajo del estudiante	<1%
6	vlex.ec Fuente de Internet	<1%
7	Submitted to Universidad Internacional de la Rioja Trabajo del estudiante	<1%
8	www.coe.int Fuente de Internet	<1%
9	fipcaec.com Fuente de Internet	<1%
10	Submitted to Consorcio CIXUG Trabajo del estudiante	<1%
11	Submitted to Universidad San Francisco de Quito	<1%

(f): JAIME EDUARDO ALVEAR FLORES — Firmado digitalmente por JAIME EDUARDO ALVEAR FLORES. Fecha: 2026.03.06 21:50:41 -0500'

DR. JAIME EDUARDO ALVEAR FLORES
TUTOR DE TRABAJO

C.C.: 100152792-6

PÁGINA DE APROBACIÓN DEL TRIBUNAL

El tribunal examinador, aprueba el presente trabajo en nombre de la Pontificia Universidad Católica del Ecuador Ibarra:

JAIME EDUARDO ALVEAR FLORES
Firmado digitalmente por JAIME EDUARDO ALVEAR FLORES
Fecha: 2026.03.06 21:51:06 -0500'

(f): .....

Dr. Jaime Eduardo Alvear Flores

C.C.: 100152792-6

Firmado electrónicamente por: JHONNY IVAN HURTADO MORENO
Validar únicamente con FirmaEC

(f):.....

Dr. Jhonny Iván Hurtado Moreno

C.C.: 100265873-8

Farid Estuardo Manosalvas Granja
Firmado digitalmente por Farid Estuardo Manosalvas Granja
Fecha: 2026.03.12 19:45:02 -05'00'

(f):.....

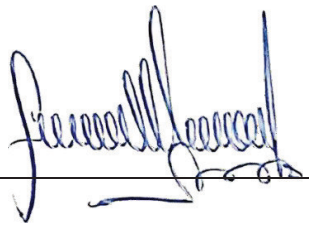
Dr. Farid Estuardo Manosalvas Granja

C.C.: 100153516-8

ACTA DE CESIÓN DE DERECHOS

Nosotros, *Anderson Mauricio Hernández Arévalo Y José Alejandro Narváez Tacuri*, declaramos conocer y aceptar la disposición del Art. 165 del Código Orgánico de Economía Social de los Conocimientos, Creatividad e Innovación, que manifiesta textualmente: "Se reconoce facultad de los autores y demás titulares de derechos de disponer de sus derechos o autorizar las utilizaciones de sus obras o prestaciones a título gratuito y oneroso, según las condiciones que determinen. Esta facultad podrá ejercerse mediante licencias libres, abiertas y otros modelos alternativos de licenciamiento o la renuncia".

Ibarra, 03 de marzo del 2026

(f): 

Anderson Mauricio Hernández Arévalo

C.C.: 100398994-2

(f): 

José Alejandro Narváez Tacuri

C.C.: 100444299-0

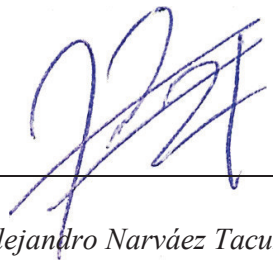
AUTORIA

Nosotros, *Anderson Mauricio Hernández Arévalo Y José Alejandro Narváez Tacuri*, portadores de las cedulas de ciudadanía N° 100398994-2 y 100444299-0 declaramos que el presente trabajo de investigación es de total responsabilidad de los autores y eximo expresamente a la Pontificia Universidad Católica del Ecuador Ibarra de posibles reclamos o acciones legales.

(f): 

Anderson Mauricio Hernández Arévalo

C.C.: 100398994-2

(f): 

José Alejandro Narváez Tacuri

C.C.: 100444299-0

DEDICATORIA

A Dios, por ser nuestra guía en cada paso de este camino, por darnos la fuerza en los momentos difíciles y por iluminar nuestro esfuerzo con su infinita sabiduría. Sin Él, este logro no tendría el mismo significado.

A nuestras familias, quienes han sido nuestro mayor soporte. Gracias por su amor incondicional, por alentarnos cuando las fuerzas flaqueaban y por creer en nosotros incluso cuando dudábamos de nosotros mismos. Su apoyo ha sido el motor que nos ha impulsado a seguir adelante.

A todas las personas que, de una u otra manera, nos han acompañado en este proceso: profesores, amigos y mentores que con sus palabras, enseñanzas y gestos de apoyo nos han ayudado a crecer y a superar cada obstáculo.

Este trabajo no es solo nuestro, sino también de todos aquellos que han estado a nuestro lado en esta etapa. A ellos, nuestro más profundo agradecimiento.

AGRADECIMIENTOS

Este trabajo de titulación no habría sido posible sin el apoyo de personas fundamentales en nuestro camino.

En primer lugar, queremos expresar nuestro más sincero agradecimiento a nuestros tutores, quienes con su guía, paciencia y conocimiento nos ayudaron a dar forma a este proyecto. Sus consejos fueron luz en los momentos de incertidumbre y su exigencia nos impulsó a dar lo mejor de nosotros.

A nuestras familias, que han sido nuestro pilar en cada etapa de este proceso, gracias por la comprensión en los días de estrés, por las palabras de aliento cuando más las necesitábamos y por recordarnos que todo esfuerzo tiene su recompensa. Su apoyo incondicional nos ha dado la fuerza para seguir adelante, incluso cuando el camino se tornó difícil.

Este logro también es de ustedes.

ÍNDICE

1. RESUMEN Y PALABRAS CLAVE

La presente investigación se titula “La Apropiación Fraudulenta por medios electrónicos: análisis del tipo penal en el COIP”, la cual se enfoca en analizar el impacto que tiene el delito de apropiación fraudulenta por medios electrónicos en el derecho constitucional a la protección de datos personales y sus implicaciones jurídicas, institucionales y financieras. En sí, este delito vulnera el derecho a la privacidad de las personas en las comunicaciones digitales, ya que los infractores utilizan datos personales para obtener beneficio propio o para terceros o simplemente venden información personal financiera a personas en el extranjero, causando un perjuicio a miles de ecuatorianos cada año. De hecho, fue desde el año 2020 que se creó en el país la Unidad Fiscal Especializada en Ciberdelitos, y a partir del año 2020 al 2022, se han registrado más de 3000 denuncias por estos casos. En este sentido, el objetivo general de la presente investigación fue analizar cuáles son las implicaciones jurídicas y financieras que el delito de apropiación fraudulenta por medios electrónicos les produce a las víctimas a nivel nacional e internacional. Se consolidó este objetivo mediante la utilización de los métodos: normativista, analítico-sintético e inductivo, llegando a obtener como principales resultados: que existe una deficiencia por la falta de más unidades de fiscalía especializadas; segundo, se analizaron dos casos emblemáticos en los que se utilizó la técnica de clonación de tarjeta de crédito y la técnica del scanning o escaneo visual de los datos financieros de una persona; y se logró evaluar la opinión de los profesionales del derecho, corroborando la información adquirida, obteniendo como conclusión, que las principales dificultades para la investigación de estos delitos es que los infractores fuera del territorio nacional, por lo que se deben aplicar convenios de Derecho Internacional Privado para juzgarlos.

PALABRAS CLAVE: ciberdelitos, apropiación fraudulenta por medios electrónicos, derecho a la protección de datos personales, delitos financieros.

2. ABSTRACT

The former research is entitled The Fraudulent Appropriation by Electronic Means: Analysis of the Criminal Offense in the COIP, which focuses on analyzing the impact of the crime of fraudulent appropriation by electronic means on the constitutional right to the protection of personal data and its legal, institutional and financial implications. In itself, this crime violates the right to privacy of individuals in digital communications, since offenders use personal data for personal gain or for third parties or simply sell personal financial information to people abroad, causing damage to thousands of Ecuadorians each year. In fact, it was since 2020 that the Specialized Cybercrime Prosecutor Unit was created in the country, and from 2020 to 2022, more than 3000 complaints have been registered for these cases. In this sense, the general objective of this research was to analyze the legal and financial implications of the crime of fraudulent appropriation by electronic means for victims at the national and international level. This objective was consolidated through the use of normative, analytical-synthetic and inductive methods, obtaining as main results: that there is a deficiency due to the lack of more specialized prosecution units; secondly, two emblematic cases were analyzed in which the technique of credit card cloning and the technique of scanning or visual scanning of a person's financial data were used; and the opinion of legal professionals was evaluated, corroborating the information acquired, obtaining as a conclusion, that the main difficulties for the investigation of these crimes is that the offenders are outside the national territory, so that conventions of Private International Law must be applied to judge them.

KEYWORDS: cybercrimes, fraudulent appropriation by electronic means, right to personal data protection, financial crimes.

3. INTRODUCCIÓN

El presente trabajo se titula: “La apropiación fraudulenta por medios electrónicos: análisis del tipo penal en el COIP”. Su objetivo es examinar el impacto que este delito tiene sobre el derecho constitucional a la protección de datos personales, así como sus implicaciones jurídicas, institucionales y financieras. Los actores principales involucrados en esta problemática son los infractores que se apropian indebidamente de datos personales y financieros, la Fiscalía, las instituciones bancarias y las víctimas de estas conductas.

La investigación surge a partir de dos situaciones concretas: primero, la creciente frecuencia con la que los ciudadanos denuncian transacciones realizadas a su nombre por terceros, mediante el uso no autorizado de tarjetas de crédito o débito; y segundo, la inseguridad que esto genera en los usuarios de servicios digitales, en especial quienes realizan compras en línea.

En esencia, este delito consiste en la utilización indebida de información financiera personal (como números de tarjetas, códigos de seguridad o datos de identidad) para ejecutar transacciones no consentidas en beneficio del infractor o de terceros, dentro o fuera del país. En Ecuador, entre 2020 y julio de 2022 se registraron 3.183 delitos informáticos, con una tendencia creciente pese a la creación de la Unidad Especializada en Delitos Informáticos, que hasta la fecha cuentan con pocas sedes, lo que limita su efectividad. Cabe señalar que esta problemática existe desde la aparición y uso de las primeras aplicaciones bancarias, plataformas de comercio electrónico y redes sociales.

Precisamente por ello, la pregunta central de investigación es: ¿Qué características define el tipo penal de apropiación fraudulenta por medios electrónicos en el Código Orgánico Integral Penal (COIP), y cómo se podrían optimizar su interpretación y aplicación para combatir este delito de manera efectiva? Y para dar respuesta a esta pregunta, es indispensable responder a tres interrogantes, que son: ¿cuáles son los elementos esenciales que componen el tipo penal de apropiación fraudulenta por medios electrónicos en el COIP,

incluyendo los aspectos técnicos y jurídicos que lo caracterizan?, ¿qué información se puede obtener del análisis de casos emblemáticos en los que se haya dictado sentencia condenatoria respecto a las dificultades en la investigación de estos delitos?, ¿Cuál es la percepción de los profesionales del derecho respecto a las implicaciones jurídicas y financieras del delito de apropiación fraudulenta por medios electrónicos?

Para dar respuesta a ello, el objetivo general de esta investigación es Analizar el tipo penal de la apropiación fraudulenta por medios electrónicos establecido en el Código Orgánico Integral Penal (COIP), evaluando sus elementos constitutivos, limitaciones legales y posibles mejoras para su correcta aplicación en el marco jurídico ecuatoriano. Esto será conseguido mediante tres objetivos específicos que son:

a) Identificar los elementos esenciales que componen el tipo penal de apropiación fraudulenta por medios electrónicos en el COIP, incluyendo los aspectos técnicos y jurídicos que lo caracterizan. La idea de este objetivo es obtener la información necesaria para contextualizar al lector acerca de la apropiación fraudulenta por medios electrónicos. Esto se realizará mediante el análisis bibliográfico, con la finalidad de que se pueda esclarecer las consecuencias jurídicas que produce esta conducta delictiva y sus formas de comisión.

b) Analizar casos emblemáticos a nivel nacional respecto al delito de apropiación fraudulenta de medios electrónicos en Ecuador. Esto con el fin de que el lector encuentre en el análisis de los casos que tienen sentencia condenatoria, las principales dificultades que existen al momento de probar este delito.

c) Evaluar la opinión de los profesionales del derecho respecto a las implicaciones jurídicas y financieras del delito de apropiación fraudulenta por medios electrónicos. Esto se realizará a través de la entrevista con el cuestionario de preguntas semi estructuradas a fin de poder encontrar en la percepción de los profesionales, las posibles falencias normativas o fácticas que existen a la hora de sancionar estos delitos.

Además, este tema en cuestión ha sido considerado por el pensamiento jurídico actual, incluso por funcionarios como la Fiscal General del Estado del Ecuador, Diana Salazar, y otros (2021) quien señala que:

> La importancia de este tema se refleja en los datos oficiales. Según Salazar et al. (2021), desde la entrada en vigencia del COIP en 2014, el Sistema Integrado de Actuaciones Fiscales (SIAF) ha registrado cifras relevantes: 829 denuncias por acceso no autorizado a sistemas informáticos, 10.393 casos de apropiación fraudulenta a través de medios electrónicos y 387 reportes de transferencia electrónica ilícita de bienes patrimoniales. Estos números muestran un aumento constante en las denuncias relacionadas con ciberdelitos.

La relevancia de esta investigación radica en visibilizar las dificultades de la Fiscalía en la persecución de estos delitos y en plantear posibles alternativas para mitigarlas, tanto a nivel institucional como en el ámbito de la educación ciudadana en materia de protección de datos personales y financieros.

Los principales beneficiarios de este trabajo son, en primer lugar, la ciudadanía, al adquirir mayor conocimiento sobre los riesgos que enfrentan en el uso de servicios digitales; y, en segundo lugar, los estudiantes de derecho y ciencias políticas, quienes podrán tomar como base este análisis para futuras investigaciones relacionadas con la política criminal y los ciberdelitos.

El presente trabajo de titulación, titulado "La apropiación fraudulenta por medios electrónicos: Análisis del tipo penal en el COIP", se enmarca dentro de la línea de investigación número 13 de la PUCE, Derecho, participación, gobernanza, regímenes políticos e institucionalidad. La elección de esta línea se justifica en función de la necesidad de analizar el marco jurídico vigente en Ecuador en relación con los delitos informáticos, así

como el impacto de la regulación penal en la gobernanza y la institucionalidad del sistema de justicia. (PUCE, 2017)

En definitiva, la apropiación fraudulenta por medios electrónicos constituye un fenómeno jurídico y social en expansión, derivado de la digitalización de los servicios financieros y la creciente dependencia de la sociedad en las tecnologías de la información. Por ello, resulta imprescindible un análisis académico que evalúe su tipificación, aplicación y vacíos legales, así como la respuesta del Estado y de las instituciones encargadas de garantizar la seguridad jurídica de los ciudadanos.

4. ESTADO DEL ARTE

El Código Orgánico Integral Penal en su artículo 190, señala que quien utilice o se apropie sin consentimiento del titular de un sistema informático o redes electrónicas para sacar un provecho de cualquier índole para sí o para un tercero, comete este delito y es sancionado con una pena privativa de libertad de 1 a 3 años. Esto implicaría utilizar los datos de una persona para realizar compras a su nombre y sin su consentimiento, lo que puede ser realizado a través del robo de información por hackeo, o a través del método *scanning*, en el que simplemente se visualiza los datos privados de una tarjeta y de su titular para hacer compras en línea haciéndose pasar por él.

Dicha conducta vulnera el derecho a la protección de datos personales reconocido en el artículo 66, numeral 19, de la Constitución de la República, el cual garantiza que los datos bajo custodia estatal o bancaria no sean utilizados sin autorización.

Ahora bien, la sanción por estos delitos no siempre existió en el Ecuador. De hecho, la primera vez que se lo tipificó fue en la Ley No. 67, publicada en Registro Oficial Suplemento 557 de 17 de abril del 2002, la cual añadía al Código Penal de 1971 el siguiente artículo:

> El artículo […] establece que quien utilice medios electrónicos, informáticos o similares para vulnerar claves o sistemas de seguridad con el objetivo de acceder o extraer información protegida, afectando la confidencialidad, el secreto o la integridad de dichos sistemas, será sancionado con una pena de prisión que va de seis meses a un año, además de una multa entre quinientos y mil dólares. En caso de que la información comprometida esté relacionada con la seguridad nacional o con secretos industriales o comerciales, la pena se incrementará de uno a tres años de prisión y la multa ascenderá a un rango de mil a mil quinientos dólares. (Asamblea Nacional, 2012)

Posteriormente, a través de la creación del Código Orgánico Integral Penal de 2014 que sustituía al de 1971 y a la mencionada Ley Reformatoria No. 067, se establece este tipo penal que hoy en día se conoce como la "Apropiación Fraudulenta por Medios Electrónicos" así se lo establece en el artículo 190, y que abarca los verbos rectores hoy en día conocidos:

> La persona que, de manera fraudulenta, haga uso de sistemas informáticos o de redes electrónicas y de telecomunicaciones con el propósito de apropiarse indebidamente de bienes ajenos, o de realizar transferencias no autorizadas de activos, valores o derechos, perjudicando al titular o a un tercero y beneficiando a sí misma o a otros, mediante la alteración, manipulación o modificación del funcionamiento de redes, programas, sistemas informáticos, telemáticos o equipos terminales, será sancionada con una pena de prisión que va de uno a tres años, conforme lo establece el Código Orgánico Integral Penal (Asamblea Nacional, 2014).

No obstante, el surgimiento y la evolución de estos delitos no puede explicarse únicamente desde la perspectiva de la normativa penal. En realidad, están estrechamente vinculados al desarrollo de las tecnologías de la información y la comunicación, que han generado nuevas oportunidades como el comercio electrónico y el uso de tarjetas de crédito o débito protegidas por datos personales. Estas innovaciones, a su vez, han traído consigo riesgos significativos para el patrimonio de las personas, entre ellos el hackeo, el scanning y otras modalidades de ciberdelincuencia.

La incorporación progresiva de las tecnologías de la información y la comunicación transformó de manera sustancial las dinámicas sociales y económicas, configurando lo que hoy se conoce como la era digital. Este escenario se caracteriza por el uso de redes sociales como medios de interacción, la implementación de aplicaciones destinadas a transacciones comerciales y la posibilidad de realizar compras en línea mediante el manejo de datos financieros personales. Se considera que la era digital tuvo sus inicios tras la Cuarta Revolución Industrial, en la década de 1980:

> La denominada Cuarta Revolución Industrial, también identificada como era digital, tuvo su origen en la década de 1980. Desde entonces, se ha producido una transición del uso de tecnologías mecánicas y electrónicas analógicas hacia soluciones digitales modernas. Este desarrollo ha estado marcado por innovaciones como la nanotecnología, la miniaturización de componentes, la computación cuántica y los avances en telecomunicaciones (Terol y Chavarri, 2023, párr. 1).

El advenimiento de la era digital y las nuevas formas de comunicación generaron también importantes desafíos en materia de seguridad, especialmente relacionados con la privacidad y la intimidad de las personas en los entornos virtuales. Plataformas como las redes sociales, las aplicaciones bancarias y otros servicios de libre acceso comenzaron a almacenar grandes volúmenes de datos personales, que incluyen desde información civil básica hasta credenciales financieras utilizadas en transacciones comerciales tanto físicas como en línea.

Ante este contexto, la delincuencia encontró mecanismos para vulnerar los sistemas de seguridad de dichas plataformas y acceder sin autorización a sus bases de datos, con el fin de obtener información que luego es utilizada para beneficio propio o de terceros. Este fenómeno constituye lo que actualmente se conoce como ciberdelincuencia.

Sobre este aspecto, Benavides et al. (2020) señalan que:

> La modernización ha traído consigo, que el manejo de la información, se realice mediante procesadores informáticos, que permiten almacenar una cantidad considerable de información y, que, al mismo tiempo, se pueda acceder de manera rápida y efectiva a esos datos. La información puede ser de cualquier tipo (personal, empresarial, financiera-bancaria, societaria), siendo esta apetecida por los llamados delincuentes informáticos con la intención de sacar provechos de tipo oneroso, por intermedios del chantaje, desprestigio y hasta secuestro de la información sustraída" (p. 354).

En consecuencia, la ciberdelincuencia se convertiría en un fenómeno delincuencial mundial, cuyos efectos negativos habrían sido percibidos por los Estados en diversas partes del mundo, entre los períodos de 1970 y 1980:

> El surgimiento de los delitos informáticos se dio de la mano con el avance de las tecnologías de la información. Uno de los primeros incidentes en la historia de Internet fue el programa Creeper, desarrollado en 1971 por el ingeniero Bob Thomas. Aunque considerado el primer virus informático, no provocó daños en los equipos afectados. No obstante, sentó las bases para ataques posteriores que sí generaron importantes pérdidas económicas. Por su parte, la Organización de Cooperación y Desarrollo Económico (OCDE) inició en 1983 un estudio destinado a promover la internacionalización de las leyes penales frente al uso indebido de software, el cual fue publicado en 1986. Este documento incluía propuestas de reformas legales, criterios normativos y una lista mínima de conductas que deberían ser penalizadas. Posteriormente, en 1992, la OCDE desarrolló un conjunto de normas técnicas con el fin de establecer un marco de seguridad para los sistemas de información (Ramírez, 2020, p. 140)

Al respecto de este ámbito temático, existen diversas investigaciones realizadas con anterioridad por otros autores, como Benavides, Acosta y García, en su obra "*Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios*" quienes señalan que:

> Los delitos informáticos constituyen conductas ilegales que se llevan a cabo a través del uso indebido de herramientas tecnológicas, afectando la confidencialidad de la información de terceros, ya sea mediante la alteración, sustracción o daño de datos almacenados en dispositivos electrónicos o servidores. (p. 351)

También conocidos como *gadgets* simplemente son pequeños dispositivos de almacenamiento, que pueden ser desde computadoras, hasta celulares, tables, discos duros, o cualquier otra forma en la que se pueda almacenar información digital en medios físicos.

Para complementar un poco la información proporcionada por los autores. Ramírez (2020) en su obra, "*Aplicación de informática forense en auditorías gubernamentales para la determinación de indicios de responsabilidad penal con delitos informáticos en Ecuador*" también brinda otra definición de lo que son los delitos informáticos:

> Los delitos informáticos se entienden como conductas ilícitas que pueden realizarse de forma intencional o por descuido, utilizando dispositivos electrónicos con fines como acceder, interceptar, eliminar, transferir, alterar o divulgar información contenida en sistemas informáticos. Estas acciones comprometen la integridad, seguridad, disponibilidad y confidencialidad de los datos. Siempre que estén contempladas en la normativa penal y sean atribuibles a los responsables de la gestión de recursos públicos, generan responsabilidad penal (p. 142).

En este ámbito, los bienes jurídicos comprometidos son diversos: la intimidad, la correspondencia, el derecho a la protección de datos personales y, de manera central, el patrimonio. La responsabilidad penal se genera siempre que la conducta se encuentre tipificada en la normativa vigente, en concordancia con el principio de legalidad.

De estos delitos, uno de ellos es la apropiación fraudulenta por medios electrónicos, que consiste básicamente en la sustracción de información personal de los usuarios (en su mayoría, financiera) para poder obtener un beneficio propio o de terceros, mediante la apropiación y hackeo de sistemas de seguridad de redes sociales, aplicaciones, etc., mediante la sustracción física o electrónica de dicha información. En sí, los verbos rectores principales son: la utilización ilegal, ilícita y no consentida por el titular, de un sistema informático,

redes electrónicas o de telecomunicaciones, para obtener un beneficio personal o para un tercero.

Cabe destacar que, al no tratarse de un delito especial, el sujeto activo no requiere cualificación particular para su comisión, por lo que puede ser perpetrado tanto por personas naturales como por entidades jurídicas de derecho público o privado.

Ahora bien, respecto a cómo se ejecutan los delitos por medios electrónicos, existen diversas formas como lo es la apropiación fraudulenta mediante hackeo e interceptación ilegal a sistemas de seguridad de aplicaciones bancarias, así como el *skimming*, y el *scanning*.

La primera y menos común es la apropiación fraudulenta mediante hackeo o interceptación ilegal a sistemas de seguridad de aplicaciones bancarias, redes sociales o plataformas de pago, en la que se sustraen bases de datos que contienen información financiera y datos personales de usuarios particulares. Es lo que se conoce como Hackeo.

Frente a estas amenazas, el Ecuador ha avanzado en la construcción de un marco regulatorio orientado a combatir los delitos cometidos por medios informáticos. La incorporación de figuras delictivas en el Código Orgánico Integral Penal (COIP) reconoce la necesidad de sancionar conductas como el acceso ilícito a sistemas, la intercepción de datos y el fraude electrónico. Sin embargo, la dinámica cambiante de la ciberdelincuencia exige no solo un marco sancionador, sino también medidas preventivas y mecanismos de supervisión eficaces.

A pesar de estos esfuerzos, la cibercriminalidad sigue representando un desafío creciente, pues los avances tecnológicos brindan nuevas oportunidades para la comisión de delitos y dificultan su detección y persecución. Por ello Enríquez, (2022), en su publicacion titulada

"*Hacia una cultura de "Valor al Riesgo" en la ciberseguridad del Ecuado*r" hace mención a lo siguiente:

> Ecuador ya dispone de una Ley Orgánica de Protección de Datos Personales, la cual exige tanto a entidades públicas como privadas que apliquen medidas técnicas y organizativas para resguardar los datos personales de los ciudadanos, conforme lo establece el artículo 37. Sin embargo, ha transcurrido más de un año sin que se concrete la creación de la Superintendencia de Datos.
>
> Asimismo, en la Asamblea Nacional se encuentran en trámite tres iniciativas legislativas sobre seguridad digital, aunque ninguna de ellas aborda el análisis cuantitativo de riesgos en materia de seguridad. La implementación de la Estrategia de Ciberseguridad podría verse truncada, como ha ocurrido con muchas otras propuestas valiosas en el pasado, por la falta de compromiso político (p. 1).

De esta manera, han existido en la historia ciertos acontecimientos que instituciones financieras locales han sido víctimas, poniendo en riesgo la seguridad de los clientes, al ser un elemento vulnerable.

Sin embargo, Harán (2021) en su boletín informativo denominado "Banco Pichincha sufrió ataque informático que afectó parte de sus servicios" afirma que esta no habría sido la única vez en la que ocurrió el incidente, debido a que, anteriormente, en febrero del año 2021, ya se había registrado otro ataque a la misma institución y al Ministerio de Finanzas del Ecuador:

> Aunque Banco Pichincha no ofreció información detallada sobre la naturaleza del incidente, y señaló que están trabajando con expertos para investigar lo sucedido, el portal *Bleeping Computer* indicó que se trataría de un ataque de ransomware vinculado al uso de la herramienta de pruebas de penetración *Cobalt Strike*,

> frecuentemente empleada por grupos cibercriminales, incluidos aquellos dedicados al ransomware.
>
> Cabe mencionar que en febrero del mismo año, la entidad bancaria ya había sufrido otro ataque informático, atribuido al grupo *Hotarus Corp*, que también afectó al Ministerio de Finanzas de Ecuador y afirmó haber sustraído información confidencial de ambas instituciones (párr. 4 y 5).

En el marco de los ataques dirigidos contra infraestructuras y servicios digitales, el ransomware ha emergido como una de las amenazas más disruptivas para la continuidad operativa y la confidencialidad de la información. A continuación, se reproduce, sin alteraciones, la descripción técnica que varios autores han consignado sobre esta modalidad manifestando que;

> El ransomware es un tipo de software malicioso que se caracteriza por bloquear el acceso a un sistema o a la información contenida en él, exigiendo al usuario el pago de un rescate para poder recuperarlos. Esta forma de ataque, que ha experimentado un crecimiento considerable en los últimos años, generalmente actúa cifrando archivos específicos mediante una clave que solo posee el atacante, quien la entrega únicamente tras recibir un pago por parte de la víctima (Trigo et al., 2017).

En contraste con el ransomware se suele apuntar a sistemas completos o repositorios de datos, el hackeo dirigido va hacia las plataformas financieras u otras aplicaciones representa una técnica compleja y de mayor sofisticación técnica. Su ejecución suele requerir conocimientos avanzados en programación, explotación de vulnerabilidades y manejo de herramientas especializadas. Por ello, aunque sus consecuencias pueden ser masivas (p. ej. extracción de bases de datos con miles de registros), el hackeo es relativamente menos frecuente que otras técnicas de extracción de datos debido a su barrera técnica de entrada. En muchos casos, la intención del atacante es obtener grandes volúmenes de información financiera para su comercialización en mercados ilícitos o para su uso en fraude transnacional.

La otra técnica accesibles y extendidas entre los delincuentes son las técnicas de skimming y scanning. El skimming consiste en la copia no autorizada de los datos contenidos en la banda magnética o chip de una tarjeta durante su uso legítimo, mediante dispositivos adulterados que retienen la información y permiten su posterior clonado o venta. Al respecto, Carrillo (2013) describe esta práctica de la forma siguiente:

> Los casos más comunes de clonación de tarjetas suelen darse en establecimientos comerciales tradicionales y cajeros automáticos, utilizando un dispositivo electrónico llamado *skimmer*. Este aparato permite copiar la información contenida en la banda magnética de la tarjeta. Luego, estos datos son procesados mediante un equipo informático y un software que captura la información y la transfiere a una tarjeta nueva, generando así una copia idéntica de la original. El término "*skimming*" se ha popularizado para describir cualquier situación en la que se roba información de tarjetas durante un uso legítimo del medio de pago (Carrillo, 2013, p. 212).

La información obtenida mediante skimming puede servir tanto para la clonación física de tarjetas como para la venta de credenciales en mercados ilegales; el comprador de dichos datos puede, a su vez, efectuar compras en línea usando identidad ajena y técnicas para ocultar su trazabilidad (por ejemplo, navegación con ocultamiento de IP o envío del bien a terceras direcciones).

En este último caso, el comprador de estas tarjetas únicamente necesitaría utilizar un número de cédula y nombre diferente al suyo, lo cual puede encontrar de varias maneras, y realizar la compra desde un ordenador que disponga de un navegador que oculte la dirección IP, lo cual implicaría que se desconozca la ubicación exacta (calles o sector) desde donde se habría realizado la compra. Incluso haciendo esto, podría pedir a la página web que le envíen la compra a alguna ubicación diferente a la suya. La investigación sobre estos delitos es muy compleja y normalmente se puede identificar al comprador de los datos financieros, pero no es fácil identificar al vendedor o persona que realmente robó los datos personales del usuario. De hecho, solo los casos en donde la persona que realiza el robo de datos, es la misma que

realiza las compras, se vuelve un poco menos compleja la tarea de identificar al infractor, pero normalmente esto no es común.

El scanning, por su parte, refiere a prácticas aún más básicas en términos técnicos pero igualmente efectivas: la captura visual o el registro directo de datos financieros a partir del acceso físico o momentáneo a la tarjeta o al dispositivo móvil de la víctima. Ejemplos típicos son la anotación de claves en notas de un teléfono robado, la observación del CVC en el momento de una transacción o la lectura de información cuando la tarjeta pasa por el alcance de un lector ilegal.

Uno de los métodos más conocidos y empleados es el método más común como el Phishing lo cual es un método de estafa o de apropiación fraudulenta basado en el engaño, que, en el caso de la apropiación fraudulenta, consiste en ofertar productos a través de páginas web para realizar compras en línea. El usuario coloca sus datos y de esa manera se le sustrae información que después es utilizada para realizar compras verdaderas por internet, haciéndose pasar por la persona:

Valle Matute (2013) en su artículo titulado, El delito Informático del Phishing, manifiesta que;

> El *phishing* es un método de ingeniería social que los delincuentes emplean para conseguir datos privados, tales como nombres de usuario, contraseñas y detalles de tarjetas de crédito, haciéndose pasar por comunicaciones legítimas y confiables (p. 30).

En el contexto ecuatoriano, estas prácticas han tenido expresiones locales. Un caso ocurrió en Babahoyo en 2022, cuando la Cooperativa de Taxis San Fernando fue víctima de un ataque de este tipo debido al uso frecuente de correos electrónicos para la recepción de

documentos. Según Galeas (2022), esta situación evidenció la vulnerabilidad de la organización y la necesidad de capacitar a su personal para prevenir ataques cibernéticos que pudieran comprometer tanto la información institucional como la de sus asociados.

Estas modalidades de fraude se encuentran actualmente reguladas en el Código Orgánico Integral Penal (COIP). Desde el 17 de febrero de 2021, el artículo 190 tipifica la apropiación fraudulenta por medios electrónicos en los siguientes términos:

> Art. 190.- Apropiación fraudulenta por medios electrónicos.- La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años. (Asamblea Nacional, 2014)

Este tipo penal sanciona la vulneración del derecho a la protección de datos personales, establecido y amparado en el artículo 66, numeral 19 de la Constitución de la República del Ecuador (2008) el cual señala que:

> Artículo 66.- Se reconoce y garantiza a las personas, entre otros derechos, el derecho a la protección de sus datos personales (19). Esto implica que los individuos tienen el control y la facultad de decidir sobre la información que les concierne, así como su adecuada protección. La obtención, almacenamiento, tratamiento, distribución o divulgación de dichos datos requerirá siempre el consentimiento del titular o estará respaldada por una disposición legal (Asamblea Constituyente, 2008).

En el contexto actual, la protección de los datos personales y la seguridad en el ciberespacio se han convertido en prioridades para los Estados. En Ecuador, el Gobierno ha implementado diversas políticas públicas orientadas a fortalecer la ciberseguridad y la lucha contra los ciberdelitos. Una de las iniciativas más relevantes en esta materia es el Acuerdo Ministerial No. 006-2021, que establece lineamientos estratégicos para garantizar un entorno digital seguro y resguardar los derechos fundamentales de la ciudadanía. A continuación, se analiza el contenido de esta política y sus principales objetivos en la prevención, investigación y sanción de los delitos informáticos en el país.

> Dentro de esta política pública, se encontraba el objetivo específico 3, el cual se relacionaba directamente con la investigación y sanción de ciberdelitos:
>
> Resguardar la seguridad pública y ciudadana en el ciberespacio, previniendo y contribuyendo a la investigación de delitos cibernéticos, para el normal desarrollo de las actividades públicas y privadas, y el ejercicio de los derechos fundamentales de la ciudadanía, en un entorno de confianza.
>
> Se mencionó además que esto iba a ser posible a través de las siguientes líneas de acción:
>
> 4.1. Proteger los activos digitales tanto públicos como privados dentro del ámbito de delitos informáticos que atenten a la seguridad ciudadana en el ciberespacio.
>
> 4.2. Fortalecer las capacidades institucionales y operativas para la prevención, previsión y respuesta ante la suscitación de ciberdelitos.
>
> 4.3. Establecer y promover mecanismos de denuncia del delito cibernético.
>
> 4.4. Adaptar el ordenamiento penal interno relativo al cibercrimen con los estándares internacionales.: (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2021, p. 39)

Hasta la actualidad, los esfuerzos normativos en el Ecuador se han concentrado en la tipificación penal de los ciberdelitos, sin que exista un fortalecimiento paralelo de las

capacidades institucionales y operativas en materia de prevención y detección temprana. La ausencia de auditorías que evalúen el impacto del Acuerdo Ministerial No. 006-2021 refleja esta limitación. En la práctica, la Unidad Especializada en Investigación de Ciberdelitos carece de mecanismos efectivos para identificar oportunamente el cometimiento de estos ilícitos, y los procesos judiciales relacionados muestran baja eficacia: pese al elevado número de causas registradas en el sistema SATJE, son escasas las sentencias condenatorias.

Otro aspecto crítico es el tiempo de detección por parte de las víctimas, quienes suelen enterarse de la vulneración de sus datos personales y financieros meses, o incluso años después de ocurrida. Esto ocurre, por ejemplo, cuando un infractor clona una tarjeta mediante skimming y realiza compras diferidas con identidad suplantada. En tales casos, el perjudicado recién tiene conocimiento al recibir su factura electrónica, momento en el cual inicia la acción penal. Sin embargo, el uso de identidades falsas o incluso de la propia identidad de la víctima complica significativamente la investigación.

A estas dificultades se suma la falta de regulación en la entrega de bienes adquiridos en línea. Empresas de mensajería como Servientrega o Tramacoexpress no exigen que el receptor coincida con el comprador, permitiendo que terceros (incluso un guardia de seguridad) reciban los pedidos. Este vacío normativo amplifica la vulnerabilidad frente al fraude electrónico.

Por ello y para evitar este tipo de situaciones, existen ciertas recomendaciones realizadas por instituciones bancarias que se deben tomar en cuenta:

> Las entidades bancarias en Ecuador recomiendan para el manejo seguro de los datos personales cambiar las contraseñas con regularidad, no utilizar la misma clave en diferentes sitios, evitar ingresar a páginas web desconocidas o sospechosas, no anotar las contraseñas en lugares accesibles y, durante transacciones presenciales, mantener siempre la tarjeta de crédito o débito a la vista.

> En caso de ser víctima de un ciberdelito, los usuarios deben actuar con rapidez, contactando a su banco para reportar cualquier actividad sospechosa y solicitar el bloqueo de sus tarjetas para evitar usos no autorizados. Además, es fundamental presentar la denuncia en la Fiscalía correspondiente para que se inicie la investigación y se identifique a los responsables. Los ciberdelitos afectan tanto a personas naturales como a personas jurídicas, incluyendo empresas del sector público y privado (Pintado, 2019, p. 9).

Ahora bien, tras este análisis resulta pertinente una revisión del derecho comparado. En el ámbito latinoamericano, Ecuador constituye un caso singular, al ser el único país que sanciona este ilícito bajo la denominación de apropiación fraudulenta por medios electrónicos y que reúne en una sola figura las diversas formas de suplantación de identidad con fines de apropiación patrimonial. Así lo dispone el artículo 190 del Código Orgánico Integral Penal (2014):

> La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años. (Código Orgánico Integral Penal, 2014)

Sin embargo, la forma más similar y en la que más se sanciona este delito es bajo la modalidad de "*Suplantación de sitios web para capturar datos personales*". Este delito, en la Ley 1273, vigente actualmente en Colombia, se sanciona con pena privativa de libertad de 48 meses (4 años) a 96 meses (8 años) por lo que las pena en el mencionado país es mucho más severa:

> Artículo 269G.- Quien, con fines ilícitos y sin autorización, diseñe, desarrolle, comercialice, venda, ejecute, programe o distribuya páginas web, enlaces o ventanas emergentes, será sancionado con prisión de 48 a 96 meses y multa equivalente a entre 100 y 1.000 salarios mínimos legales mensuales vigentes, siempre que su conducta no corresponda a un delito con una pena mayor. Asimismo, se aplicará la misma pena a quien altere el sistema de resolución de nombres de dominio para redirigir al usuario a una dirección IP distinta, con la intención de hacerle creer que está accediendo a su banco u otro sitio confiable, salvo que el hecho esté contemplado en un delito con sanción más severa. Si el infractor involucra a otras personas para cometer el delito, la pena podrá incrementarse entre un tercio y la mitad (Congreso de Colombia, 2000).

De igual manera, en El Salvador, la Ley Especial contra Delitos Informáticos y Conexos del año 2009, configuraba las acciones de ciberdelincuencia a las que se hace referencia en el tipo penal denominado "Interferencia en el Sistema Informático", estableciendo penas igual de semejantes que las de Colombia:

> Artículo 6.- Quien de manera intencional y por cualquier método interfiera o modifique el funcionamiento de un sistema informático, ya sea de forma temporal o permanente, será sancionado con una pena de prisión que va de tres a cinco años. Esta sanción se considera más severa si la interferencia afecta programas o sistemas informáticos públicos, o aquellos destinados a servicios de salud, comunicaciones, suministro y transporte de energía, transporte público u otros servicios públicos, así como servicios financieros, en cuyo caso la pena de prisión será de tres a seis años. (Asamblea Legislativa de la República de el Salvador, 2016)

En cambio, en Costa Rica en la Ley N° 9048 del 2012 se sanciona este delito con la misma pena que en Ecuador, pero también bajo la denominación de "*suplantación de páginas electrónicas*":

Art. 233. Se impondrá pena de prisión de uno a tres años a quien, en perjuicio de un tercero, suplante sitios legítimos de la red de Internet. La pena será de tres a seis años de prisión cuando, como consecuencia de la suplantación del sitio legítimo de Internet y mediante engaño o haciendo incurrir en error, capture información confidencial de una persona física o jurídica para beneficio propio o de un tercero. (Asamblea Legislativa de la república de Costa Rica , 2012)

Sin embargo, ninguno de estos países ha realizado auditorías especializadas referentes a los resultados de estas leyes, pero es necesario comprender que la severidad de las penas no garantiza mayor protección del derecho a la protección de datos de las personas ni menos incidencia a la comisión de estos delitos. Si bien es cierto que Colombia, el Salvador y Costa Rica sancionan estos delitos con una mayor pena, esto no se refleja necesariamente en un resultado positivo que disminuya el cometimiento de este delito.

5. MATERIALES Y MÉTODOS

La presente investigación se realizará mediante un diseño de estudio de dos casos emblemáticos que han tenido sentencia a nivel nacional en el delito de apropiación fraudulenta por medios electrónicos. Lo que se realizará es la obtención y análisis de información referente a los hechos, las pruebas y el razonamiento jurídico aplicado por el juez en cada caso.

Esto es posible a través de un enfoque cualitativo, ya que primero se obtendrá información referente a los elementos constitutivos del tipo penal (sujeto activo, sujeto pasivo, conducta ilícita, bien jurídico lesionado y formas de comisión), a través de la doctrina. Luego, con esta información y teniendo claro el panorama relacionado a la forma en la que se comete este delito, se analizarán los casos mencionados y esa información se contrastará finalmente con la opinión de expertos en el tema.

Por estos motivos, la investigación tiene un nivel de profundidad de tipo jurídico-descriptivo, dado que se describe y narra la forma en la que se cometen estos delitos y se visibiliza la realidad de estas conductas ilícitas a través de los hechos analizados en los tres casos emblemáticos.

Para ello se utilizará el método Analítico, ya que este tendrá el objetivo de establecer y aclarar la tipificación del delito del tipo penal que se suscita al cometimiento o ejecución de un acto delictivo el cual es tipificado como tal, de igual forma se hará el uso del método Socio-jurídico, ya que aportará a un estudio más eficaz a la investigación en la cual se hará un análisis en relación al servicio que presta la entidad financiera hacia el cliente y esta misma qué tipo de responsabilidades tiene en caso de que el sujeto pasivo sea víctima por algún delito cometido por un medio electrónico y el método exegético dará un aporte, porque fue necesario investigar ciertos casos en donde se presenta los fenómenos y efectos sociales que se generan ya que se tiene que conocer cuál es la cultura y conocimiento de este tema en la sociedad para ello él es importante la utilidad estos métodos para reforzar la

investigación ya que aplicará ciertos instrumentos de apoyo como la entrevista la cual se destinará a los profesionales del derecho que prestaban servicio en entidades financieras específicas, ya que por su nivel de preparación profesional tienen un amplio conocimiento respecto al tema.

Se desarrollará como instrumento de investigación, la entrevista, la cual tiene como finalidad, responder a las inquietudes planteadas respecto al tipo penal materia de estudio de la presente investigación, así como su forma de comisión y si la norma es o no suficiente para cumplir los fines de prevención general del cometimiento de este ilícito.

La elección de las personas entrevistadas obedeció a criterios de muestreo no probabilístico de tipo intencional u opinático, siendo éstos la experiencia en el campo de la asesoría jurídica de entidades financieras. Para tener una visión más general, se seleccionaron a dos profesionales del derecho que prestaron sus servicios en diferentes entidades que son en un banco y la fiscalía.

Los profesionales responden a los nombres de, Dr. Sergio Peralta Armas – Asesor jurídico Banco del Pacifico y el Dr. Alex Rubén Benítez Veloz – Fiscal prestando servicios profesionales en la Fiscalía General del Estado FEDOTI 1.

6. RESULTADOS Y DISCUSIÓN

En este capítulo se presentan los resultados obtenidos a partir del análisis cualitativo realizado, orientado a responder los objetivos específicos de la investigación. Los resultados se estructuran en torno a tres ejes principales: los elementos esenciales del delito de apropiación fraudulenta por medios electrónicos previsto en el artículo 190 del Código Orgánico Integral Penal (COIP), el análisis de casos emblemáticos a nivel nacional relacionados con este tipo penal y la percepción de los profesionales del derecho sobre las implicaciones jurídicas y financieras derivadas de este delito.

Los hallazgos presentados en este apartado buscan aportar una comprensión más profunda sobre la problemática abordada, mediante la identificación de patrones, análisis de tendencias y reflexiones derivadas de la recopilación y el tratamiento de información cualitativa. Este capítulo constituye un insumo clave para la discusión, conclusiones y recomendaciones de la investigación.

6.1.1. Elementos esenciales del delito de apropiación fraudulenta por medios electrónicos, previsto en el artículo 190 del Código Orgánico Integral Penal

El delito de apropiación fraudulenta por medios electrónicos se encuentra tipificado y sancionado en el artículo 190 del Código Orgánico Integral Penal, y se caracteriza fundamentalmente por la utilización fraudulenta o sin consentimiento de sistemas informáticos, redes electrónicas o datos comerciales para la apropiación no consentida de bienes o derechos en perjuicio del legítimo titular de ese sistema informático o cuenta bancaria:

> Art. 190.- Apropiación fraudulenta por medios electrónicos.- La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de

> una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años. La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes (Asamblea Nacional, 2014)

El mencionado tipo penal contiene una serie de elementos que deben ser analizados de forma individual a fin de profundizar respecto a quienes cometen estos delitos, contra quienes se cometen estos delitos, a qué bienes jurídicos afecta esta conducta, entre otras cuestiones.

Para empezar, es necesario entender que este tipo penal corresponde a una clasificación de delito común, lo que, de acuerdo a la doctrina, significa que el sujeto activo no necesita reunir una serie de características especiales para que la conducta le sea imputable (como ocurre con los delitos especiales propios e impropios):

> En los delitos ***comunes***, el tipo penal no requiere una característica específica para que una persona sea considerada autora del delito; por lo tanto, cualquier individuo que cumpla con las condiciones generales de responsabilidad puede ser imputado como autor. Sin embargo, esta situación cambia en los delitos ***especiales***, donde la ley penal exige que el autor posea una cualidad particular. Dentro de estos delitos especiales se distinguen dos tipos: los delitos especiales propios y los impropios. En los primeros, la cualidad especial es un elemento fundamental para aplicar la pena (como ocurre con la condición de juez o fiscal en el delito de prevaricato), mientras que, en los segundos, dicha cualidad solo sirve para aumentar la gravedad de la sanción (por ejemplo, cuando un funcionario público comete la violación a la intimidad, lo que agravará la pena) (LP. Pasión por el Derecho, 2021, párr. 14 y 15).

Sin embargo, pese a tratarse de un delito común de acuerdo al art. 190 del Código Orgánico Integral Penal, el sujeto activo en este delito puede cumplir una serie de características: o bien puede ser una persona que no tenga ninguna experticia en informática y que solo haya sido capaz de visualizar información comercial privada (como la clave de una tarjeta de crédito o débito y la cédula de identidad del titular) y utilizando esa información, realice transacciones bancarias haciéndose pasar por el titular y sin su consentimiento; o bien puede ser alguien que sepa manejar dispositivos que puedan obtener claves de tarjetas de crédito o débito o que sean capaces de clonar estas tarjetas o extraer información privada necesaria para efectuar transacciones comerciales. Estos dispositivos pueden llegar a ser dos los *skimmer* o *shimmers*. Respecto al primero, Trevino (2023) señala que:

> Un «skimmer» de tarjetas de crédito es un dispositivo que un atacante de amenazas conecta a un lector de tarjetas real. Los cibercriminales suelen utilizar «skimmers» en cajeros automáticos no bancarios y en los surtidores de combustible de las gasolineras. (párr. 1)

Estos dispositivos, de acuerdo con la misma autora, extraen la siguiente información:

> Cuando el «skimmer» escanea la tarjeta de crédito de una víctima, roba la siguiente información:
>
> - Nombre del titular de la tarjeta
> - Número de tarjeta
> - Fecha de vencimiento
> - Código de verificación de tarjeta (CVC)
>
> Una vez que se obtiene esta información, se envía al atacante a través de Bluetooth. El atacante puede hacer lo que quiera con la información de la tarjeta robada. (Trevino, 2023, párr. 6 y 7)

Por otro lado, los *shimmers* son dispositivos pequeños que se colocan en el interior de las tarjetas de crédito y no son visibles desde el exterior, lo que los hace más peligrosos. Sin embargo, tienen el mismo objetivo que el *skimming*, extraer información de las tarjetas para clonarlas o realizar transacciones fraudulentas:

> La principal diferencia entre un «skimmer» de tarjetas de crédito y un «shimmer» de tarjetas de crédito es que los «skimmers» se sitúan encima de los lectores de tarjetas reales y solamente leen la banda magnética (la banda negra del reverso de la tarjeta de crédito) cuando usted pasa la tarjeta. Los «shimmers» se colocan en el interior de los lectores de tarjetas. Los «shimmers» son dispositivos muy delgados en comparación con los «skimmers» y no se pueden ver desde el exterior. A diferencia de los «skimmers», los «shimmers» solo funcionan cuando una persona inserta su tarjeta en un lector de tarjetas, ya que funciona escaneando el chip de una tarjeta de débito o crédito para robar su información.
>
> Si bien los «skimmers» y los «shimmers» funcionan de forma diferente, su objetivo es el mismo: escanear y robar la información de la tarjeta de débito o crédito de una persona para que un atacante pueda utilizarla con fines maliciosos. (Trevino, 2023, párr. 3 y 4)

En el ámbito de la apropiación fraudulenta por medios electrónicos, el sujeto activo también puede ser una persona con conocimientos en informática suficientes para la creación y propagación de virus o malware. Estas herramientas permiten la extracción ilícita de información privada, especialmente de carácter comercial o financiero, generalmente cuando la víctima descarga sin advertirlo archivos maliciosos desde páginas web fraudulentas.

De igual manera, el sujeto activo puede ser un desarrollador de sitios web falsos que simulan pertenecer a entidades bancarias o comercios en línea. En estos casos, la víctima ingresa sus

credenciales y datos de pago creyendo interactuar con una plataforma legítima, lo que facilita su posterior utilización fraudulenta.

En síntesis, el modus operandi del sujeto activo es variado y no requiere de una cualidad específica: cualquier persona que, a través de dispositivos electrónicos, programas maliciosos o páginas falsas, logre acceder a datos vinculados con tarjetas de crédito o sistemas informáticos para darles un uso fraudulento, puede ser autora de este delito.

Ahora bien, respecto al sujeto pasivo o víctima, es necesario mencionar que dentro del proceso penal, a nivel general, la víctima es el titular del derecho conculcado o lesionado:

> Por lo que merece clarificar que el sujeto pasivo es el titular del bien jurídico protegido; que la víctima es la persona afectada inclusive directamente por el hecho delictivo, la misma que bien no puede ser el sujeto pasivo, ni ser la persona titular del bien jurídico protegido y lesionado como consecuencia del ilícito penal.

> La víctima es la persona que ha sufrido daños en su integridad física o mental, en su patrimonio o cuando sus derechos fundamentales se ven afectados sustancialmente. "El concepto de víctima resulta más criminológico que jurídico, es decir, la víctima es aquella persona a quien se causa un daño individual o colectivo, físico o mental, patrimonial o moral. (Andrade, 2015, párr. 12)

Dentro de este delito, la víctima directa viene a ser cualquier persona que sea titular del sistema informático o redes electrónicas y de telecomunicaciones o cuenta bancaria, pero, además, existe otra víctima indirecta que es la sociedad en general, dado que al momento en el que se producen estas transacciones fraudulentas, sobre todo a través de virus o sitios web fantasmas, se ataca un bien jurídico que va más allá del patrimonio individual, el cual es la fe en las transacciones bancarias. Si este fenómeno se repite en la sociedad, es muy probable

que las personas en general dejen de realizar compras en línea, lo cual también afecta a las empresas que realizan sus ventas de manera honesta y prolija.

En este sentido, la conducta delictiva de la que se habla en este delito, el hecho de apropiarse fraudulentamente de estos medios electrónicos y hacer uso de ellos sin consentimiento del titular y en beneficio de terceros o propio, afecta a tres bienes jurídicos que son: el patrimonio individual del titular de estos medios electrónicos; la buena fe en las transacciones bancarias como bien jurídico colectivo (de la sociedad); el derecho a la identidad (por la falsificación de la identidad que se produce al momento de hacerse pasar por otra persona para realizar la transacción comercial); y el derecho a la protección de datos personales, consagrado en el artículo 66, numerales 19 y 20, de la Constitución de la República del Ecuador, el cual señala que:

> Art. 66.- Se reconoce y garantizará a las personas:
>
> 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.
>
> 20. El derecho a la intimidad personal y familiar.

Precisamente por este motivo, el Código Orgánico Integral Penal ha establecido que la pena privativa de libertad prevista para este tipo penal es de uno a tres años. En este sentido, hay que señalar que usualmente cuando estas actividades ocurren, si bien se restituye el patrimonio individual de la persona y se la indemniza por concepto de daños materiales e inmateriales dentro de la reparación integral (art. 78 del COIP), el perjuicio causado a la sociedad en cuanto al quebrantamiento de la buena fe en transacciones bancarias, suele ser mucho mayor al que se piensa, ya que se genera toda una cadena de efectos sociales.

En primer lugar, al vulnerarse la fe en transacciones comerciales en línea, se crea un miedo colectivo en los individuos de realizar compras en línea, lo cual genera a su vez otro perjuicio y es específicamente a quienes realizan ventas y ofertas de productos de forma lícita por internet, por lo que esta conducta también afecta el patrimonio de terceras personas; y además, atenta también con la capacidad que tiene el Estado de cumplir con la misión de proteger derechos constitucionales (derecho a la protección de datos personales) e identificar a los responsables de su vulneración.

En este sentido, quizá este delito no solo deba tener una pena privativa de libertad de uno a tres años, sino tal vez de tres a cinco años, además de una pena pecuniaria que debería ser calculada (además de la reparación integral) de acuerdo al perjuicio que cause en la sociedad y en los sectores específicos a los que haya atacado (locales de ropa, compra-venta de suplementos, de libros, o de artículos que no son de fácil acceso a nivel nacional). Solo así, se podría hablar del cumplimiento del principio de proporcionalidad establecido en el numeral 6 del artículo 76 de la Constitución de la República del Ecuador:

> Art. 76.- En todo proceso en el que se determinen derechos y obligaciones de cualquier orden, se asegurará el derecho al debido proceso que incluirá las siguientes garantías básicas: (…)
>
> 6. La ley establecerá la debida proporcionalidad entre las infracciones y las sanciones penales, administrativas o de otra naturaleza. (Asamblea Constituyente, 2008)

De hecho, si se compara con otras legislaciones, este delito suele ser sancionado con más severidad en torno al perjuicio causado. Por ejemplo, la Ley 1273 de 2009 en Colombia (vigente actualmente) sanciona en el artículo 269F, el delito de violación de datos personales, que viene a ser en Ecuador, el equivalente a la apropiación fraudulenta por medios electrónicos. Este ilícito, en la legislación colombiana, es sancionado con pena privativa de libertad de 4 a 8 años, y una pena pecuniaria de 100 a 1000 salarios básicos unificados:

> Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes. (Congreso de Colombia, 2000)

Precisamente por ello, es que, atendiendo al perjuicio causado en la sociedad, en el Estado, y en el titular de los datos personales, en función del principio de proporcionalidad, se sugiere una reforma al art. 190 del COIP, estableciendo una pena privativa de libertad de 3 a 5 años y una pena pecuniaria de 100 a 1000 salarios básicos unificados del trabajador en general.

Finalmente, en relación a los verbos rectores de este tipo penal, lo que se sanciona es la utilización fraudulenta (sin consentimiento del titular y haciéndose pasar por él/ella) de 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, lo cual, como se mencionaba antes, se consuma al momento en el que se realiza la compra fraudulenta con los datos personales del titular, se efectúa la transferencia sin el consentimiento del titular, o el sujeto activo logra apropiarse del bien o patrimonio de cualquier manera a través del uso de dispositivos o mediante el robo físico de información, lo que implica que el sujeto activo sustrajo la tarjeta de crédito o débito y la cédula del titular, obtuvo la información que necesitaba y realizó compras utilizando medios electrónicos sin el consentimiento del mismo.

Al hablar de medios electrónicos, se hace referencia a plataformas de compra-venta falsas, páginas web donde se ofertan productos de empresas (que sean verdaderas, pero que quien realiza la compra, sea un sujeto distinto al titular de la tarjeta); o incluso transferencias entre instituciones bancarias legítimas, cuando éstas fueron realizadas de forma fraudulenta (sin

consentimiento del titular). En definitiva, los medios electrónicos son todas aquellas plataformas o mecanismos virtuales o en línea que pueden ser utilizados para la obtención de bienes, la realización de transacciones comerciales y la realización de operaciones de compra-venta en línea, por lo que, al apropiarse de las mismas, al manipular o modificar el funcionamiento de estas redes electrónicas y hacerlo sin consentimiento del titular, se estarían cumpliendo los verbos rectores del delito de apropiación fraudulenta por medios electrónicos.

6.1.2. Análisis de casos emblemáticos a nivel nacional respecto al delito de apropiación fraudulenta de medios electrónicos en Ecuador

a. Análisis del caso Gaibor, No. 09281201802880, vía procedimiento abreviado, por el delito de apropiación fraudulenta de medios electrónicos

Es el caso que el día viernes 29 de junio de 2018, a las 17: 30, el señor Gaibor Zurita Klever Mauricio, se había percatado de que, en su correo electrónico, jun_azul8 @hotmail.com, había un mensaje en el que se detallaba que él habría realizado gastos ese día de 200$ y 300$ de su tarjeta *Pacificard*, No. 5110540 173705089XXX, lo cual era evidentemente falso. En ese momento, decidió llamar al Banco del Pacífico para que bloqueen la tarjeta.

Acto seguido, se aceró al Hipermarket (Mi Comisariato) del Mall Riocentro Sur de Guayaquil, lugar donde presuntamente se habrían realizado los gastos con su tarjeta de crédito. La compra se había realizado sin que se verificase la cédula del titular, únicamente otorgándole a la persona que le atendió en caja, una tarjeta clonada haciendo uso de los datos personales financieros obtenidos por un dispositivo *skimmer*. Fue por este motivo que llamó a la policía, y en compañía de los oficiales, procedieron a la revisión de las cintas de seguridad del almacén en la hora en la que se había realizado la compra (esta información fue obtenida gracias a los detalles de la compra que le llegaron al señor en el correo electrónico).

Para su sorpresa, el sujeto seguía en el mall, razón por la que uno de los agentes de policía lo reconoció y lo aprehendió, encontrándole en tenencia de las siguientes evidencias: "una laptop (computadora), 4 teléfonos celulares, un lector de tarjeta electrónica y varias tarjetas de instituciones bancarias que fueron ingresadas con la respectiva cadena de custodia, parte policial está suscrito por el agente aprehensor Felix Mora y otros" (Caso Gaibor, apropiación fraudulenta por medios electrónicos, 2018), por lo que el procesado, que responde al nombre de Escobar Sánchez Byron Michael, habría utilizado la tarjeta de la víctima para realizar la compra.

En vista de la situación, existiendo tantas pruebas en su contra y siendo aprehendido en delito flagrante, el sujeto decidió acogerse al procedimiento abreviado. En sí, las pruebas para determinar la existencia material de la infracción y la responsabilidad de la persona procesada, eran las siguientes:

Respecto a la existencia material de la infracción, primero, como prueba pericial se encuentra la copia certificada del parte de aprehensión, en el que se detalla las evidencias encontradas en el bolsillo y mochila del procesado, y que luego fueron trasladadas en cadena de custodia. Como se mencionó antes, el lector de tarjeta electrónica era falso, ya que en realidad era el dispositivo que se utiliza para la modalidad de robo digital de datos llamada "*skimming*" y "scanning", las cuales consisten en lo siguiente:

> Tanto el *skimming* como *scanning* son técnicas de lectura rápida […] en el contexto del robo de datos bancarios, *skimming* y *scanning* se refieren a técnicas utilizadas por los delincuentes para obtener información de las tarjetas bancarias.
>
> […] el skimming se refiere al uso de dispositivos ilegales para copiar la información de la banda magnética de una tarjeta bancaria. Los delincuentes colocan dispositivos de skimming en cajeros automáticos o en otros lugares donde se utilizan tarjetas bancarias. Estos dispositivos pueden copiar la información de la tarjeta, incluyendo

> el número de cuenta y la información de seguridad, y luego los delincuentes utilizan esta información para hacer compras fraudulentas o para realizar retiros de dinero.
>
> Por otro lado, *scanning* se refiere a la práctica de mirar rápidamente los recibos de las transacciones realizadas con tarjetas bancarias para obtener información útil. Los delincuentes pueden buscar en los recibos información como el número de cuenta, la fecha de vencimiento y el código de seguridad para utilizar esta información en actividades fraudulentas (Banco Compartamos, 2023, párr. 4, 5 y 6)

En el presente caso, al señor Escobar Sánchez Byron Michael no solamente se lo había encontrado con tarjetas de crédito que después se verificó que eran clonadas y que obviamente no le pertenecían a él, sino que también se pudo evidenciar que poseía un lector falso de tarjetas de crédito, dispositivo que se llama *skimmer*. Éste sería el dispositivo del que se habla en la cita respecto al "*skimming"*, ya que serviría para obtener el código de seguridad de la tarjeta de crédito y los datos personales de la misma. En sí, esto se logra porque el dispositivo logra escanear el CVC:

> El código CVV o CVC es un grupo de 3 o 4 números situado en el reverso de la tarjeta de crédito o débito. Dicho código se utiliza como método de seguridad en transacciones en las que la tarjeta no está físicamente presente, como en compras por teléfono o internet. (BBVA , 2023, párr. 1)

Con esta información, el sujeto activo del delito no solo puede realizar compras apropiándose fraudulentamente de los datos personales de la víctima por medios electrónicos, sino que también puede vender dicha información por el mercado negro a personas en el extranjero.

De hecho, ésta es otra de las maneras de operar de quienes realizan estas actividades e implica mucho menos riesgo, pues, por lo general, los compradores suelen ser personas en otros países que realizan compras por internet fuera del territorio del titular de la tarjeta y desde otros ordenadores que no sean los suyos, o dispositivos cuya dirección IP se suele perder o no es visible, por navegadores especiales que realizan esta tarea:

> Una dirección IP es una dirección única que identifica a un dispositivo en Internet o en una red local. IP significa "protocolo de Internet", que es el conjunto de reglas que rigen el formato de los datos enviados a través de Internet o la red local.
>
> En esencia, las direcciones IP son el identificador que permite el envío de información entre dispositivos en una red. Contienen información de la ubicación y brindan a los dispositivos acceso de comunicación. Internet necesita una forma de diferenciar entre distintas computadoras, enrutadores y sitios web. (Kaspery Security, 2023, párr. 1 y 2)

En la era digital, el crimen ha encontrado nuevos caminos para operar, burlando con facilidad los controles tradicionales de la justicia. En Ecuador, la Fiscalía General del Estado enfrenta una batalla desigual contra los delitos electrónicos, donde la falta de herramientas tecnológicas especializadas y una normativa en constante evolución limitan su capacidad de acción. Mientras los delincuentes aprovechan el anonimato y la rapidez del mundo digital, la persecución penal avanza con obstáculos burocráticos y técnicos que impiden respuestas eficaces. Esta brecha entre la ley y la tecnología no solo retrasa la justicia, sino que deja a las víctimas en una brecha de impunidad.

> En la legislación ecuatoriana se realiza la comparación del código penal anterior con el actual COIP, si bien hemos coincidido con varios autores que las TlCs en el campo del derecho es lo nuevo en cuanto cyber crimines, se refleja a la vez que existen diferencias entre ambas legislaciones debido a que ahora en nuestro código actual se tipifica y sanciona de manera más fuerte a quien transgreda la tranquilidad de

> correspondencia. De identidad digital, de hurtar a través de medios electrónicos, de clonar tarjetas de crédito. (Villón, 2019)

> Un inconveniente para la investigación radica en que Ecuador no cuenta con convenios internacionales que faciliten el cruce de datos informáticos -como los que existe entre Estados Unidos y Europa-. Por ello, hay complicaciones en detectar las cuentas o las direcciones IP desde las que se habría realizado el ataque o la sustracción de información personal ante las formalidades y la virtualidad de los procesos puede tardarse meses. (Fiscalía General del Estado, 2015, párr. 1, 2 y 3)

De hecho, hay un caso descrito brevemente por el fiscal en el que una mujer ingreso ciertos datos de su tarjeta en una página web para realizar compras en línea, pero que después le llegaron notificaciones de compras realizadas con dichos datos en otro país, que ascendían a 2500$:

> Uno de los casos de delito informático se registró en mayo del 2014, Diana (nombre protegido) se preguntaba: "¿Cómo consiguieron mis datos?". Solo recuerda que ingresó sus datos para realizar una compra por Internet, porque se ofrecían descuentos en productos de belleza. Lo único cierto es que la persona que usó su información le endeudó en 2.500 dólares, a través de débitos de su tarjeta. Su caso es investigado por la Fiscalía.

> En el caso de Diana, si hubiese estado vigente el COIP y se descubriera a la persona que robó sus datos, este podría recibir una pena de uno a tres años de cárcel. La persona que sustrajo la información de Diana compró por Internet dos celulares, una memoria externa y una Tablet. La joven tiene una deuda que paga en cuotas mínimas porque su sueldo no le alcanza para cubrir más montos. (Fiscalía General del Estado, 2015, párr. 4 y 5)

Ahora bien, continuando con la existencia material de la infracción, las otras pruebas fueron las siguientes: primero, Copia certificada de la denuncia presentada por la víctima ciudadana GAIBOR ZURITA KLEBER MAURICIO; segundo, copia certificada del comprobante de ingreso de evidencia cuyas evidencias Nro. 771-C (en el que consta que ingresaron las mismas evidencias antes mencionadas, que son las tarjetas, los celulares, la laptop y el lector de tarjetas); tercero, Copia certificada del informe pericial de reconocimiento de evidencias Nro. DCIT1803486, elaborado por el policía perito Mervin Montero; y cuarto:

> Copia certificada del informe investigativo Nro. 5330-2018 elaborado por el policía Luis Caicedo en que consta un mapa situacional, laminas fotográficas del lugar de la aprehensión del ciudadano, láminas de las evidencias, datos de biométrico del procesado, los antecedentes del procesado, laminas fotográficas de las evidencias, reporte de ARCOTEL de los teléfonos celulares. (Caso Gaibor, apropiación fraudulenta por medios electrónicos, 2018)

Respecto a la responsabilidad de la persona procesada, se cuenta con: primero, copia certificada del parte de aprehensión en el que se relatan las circunstancias de la aprehensión del procesado ESCOBAR SANCHEZ BYRON MICHAEL y se detalla que el policía reconoce al sujeto por las cámaras de seguridad y la hora a la que se habría realizado la presunta compra; segundo, La versión libre y voluntaria del policía aprehensor Felix Mora que se ratifica en el parte de aprehensión; y, finalmente, la aceptación del procesado ESCOBAR SANCHEZ BYRON MICHAEL de forma libre y voluntaria reconociendo su responsabilidad en el hecho cometido.

Por todo el acervo probatorio y porque afortunadamente, la persona procesada, realizó la compra dentro de un sitio que estaba fácilmente al alcance de la víctima, y traía consigo todos los dispositivos con los que habría cometido la infracción y otras infracciones pasadas que jamás fueron denunciadas (por el número de tarjetas con el que fue encontrado que no le pertenecían a él, y el escaneador de datos de seguridad de tarjetas de crédito con apariencia

de lector común de tarjetas), fue sencillo para la fiscalía obtener todos los elementos de convicción para destruir cualquier duda existente sobre la responsabilidad de la persona procesada, quien finalmente por acogerse al procedimiento abreviado, fue sentenciado por el juez con una pena privativa de libertad de 6 meses y multa de cinco salarios básicos del trabajador en general, además de una reparación integral de 500 $ que el condenado debía pagar a la víctima (lo cual hizo en la misma audiencia), siendo así que culmina el presente caso, habíendose afectado el derecho de la víctima a la protección de sus datos personales y a la intimidad, al patrimonio, pero habiendo resarcido dicho daño con la reparación integral.

Sin embargo, la pregunta gira en torno a qué hubiera pasado si el procesado no hubiera realizado las compras en un lugar al alcance de la víctima sino que lo hubiera hecho a través de internet y en un computador que no era el suyo, por medio de un navegador que ocultaba la dirección IP (y, por tanto, la ubicación desde donde se habría conectado el sujeto activo del delito), o qué hubiera pasado si es que el procesado vendía la información personal financiera obtenida con el lector de tarjetas a una persona en el extranjero por medio del mercado negro, y ésta persona habría realizado la compra fuera del país y por internet. Probablemente la causa seguiría en investigación previa por un año, y al no encontrarse elementos de convicción suficientes, se archivaría, lo cual generaría un agravio para la víctima de seguir teniendo que pagar por deudas en compras que jamás realizó; y este agravio traería consigo otro tipo de consecuencias.

b. Análisis del caso Zambrano, No. 09284201701374, por el delito de apropiación fraudulenta de medios electrónicos, judicializado en el año 2019

Es el caso que el día 6 de septiembre del año 2016, al señor Raúl Santiago Ibarra Zambrano, le llegan notificaciones vía correo electrónico respecto a consumos que él jamás había realizado con su tarjeta de crédito *MasterCard International*.

El señor entonces realizó la respectiva denuncia ante Fiscalía ese mismo día y además acudió al Banco del Pacífico para que les dieran respuesta respecto a dichos consumos y se supo que habían sido realizados en un portal denominado *Cuponcity* en la ciudad de Guayaquil, comprando masivamente tickets para atención en un spa denominado *THAI MASSAGE & SPA*, siendo el valor de la compra, de 2132,83 $.

Así las cosas, después de requerir al spa donde presuntamente se habrían realizado los gastos no consentidos, se obtuvo que quien había realizado esos gastos utilizando los datos personales financieros del señor Zambrano, habría sido la señora Andrea Lissette Espinoza Narváez, por lo que se realizó la audiencia de formulación de cargos, iniciándose el proceso penal; y, posteriormente el 24 de noviembre de 2017, se realizó la audiencia de evaluación y preparatoria de juicio, siendo así que, finalmente, la audiencia de juicio se celebró los días: 25 de junio de 2018 y 26 de marzo de 2019. En dicha audiencia, se logró demostrar la existencia material de la infracción y la responsabilidad de la persona procesada.

En cuanto a la existencia material de la infracción, se logró evidenciar: primero, accediendo al correo electrónico de la víctima, que la compra habría sido realizada en *THAI MASSAGE & SPA*, para un tratamiento de Luz Pulsada Intensa (en adelante, IPL) para rejuvenecimiento y cuidado de la piel; segundo, Fiscalía requirió un oficio solicitando información al Spa, en el que se señalara quién había realizado la compra y con qué datos lo habría hecho, encontrando así que la compradora fue Andrea Lissette Espinoza Narváez, quien no habría realizado la compra directamente con la institución, sino con *Cuponcity*, mediante la compra de una tarjeta que le daba acceso a los servicios del spa, y que la compra era del mencionado tratamiento, por el valor de 2132,83 $; tercero, el informe del Banco del Pacífico, contestando el requerimiento de Fiscalía respecto a las compras realizadas desde la cuenta de la víctima, detallando el día y el monto de dichas compras y el sitio web en el que se realizaron; y cuarto, la pericia informática realizada en el antiguo lugar de trabajo de la procesada, en la que se determina que la compra que fue realizada en *Cuponcity*, se la hizo desde el usuario de Windows de la señora Andrea Lissette Espinoza Narváez.

En cuanto a la responsabilidad de la persona procesada, las pruebas fueron las siguientes: primero, el testimonio de la víctima, el señor Raúl Santiago Ibarra Zambrano, quien manifiesta que él trabajaba en el Ministerio de Salud, especialmente en el dispensario de salud No. 12, mismo lugar en el que también trabajaba la procesada, por lo que era su compañera, y que él, como médico, estaba ocupado todo el tiempo y a veces dejaba su billetera y sus estados de cuenta encima de la mesa de trabajo en la que también se encontraba la procesada, quien habría colaborado con el señor como ayudante de farmacia o secretaria. Incluso había señalado que los abogados de ella habían querido arreglar con el señor en una ocasión de manera extrajudicial, diciéndole que le iban a dar 2500$ al señor para que no llevara el juicio adelante: "Una sola ocasión los abogados de ella quisieron arreglar con $2.500,00, yo dije que sean 5.000,00" (Caso Zambrano, apropiación fraudulenta por medios electrónicos, 2019).

La segunda prueba de la responsabilidad fue el testimonio de la Ing. Wendy Erika Viteri Sánchez, administradora del spa *THAI MASSAGE & SPA,* quien corroboró que la señora Andrea Lissette Espinoza Narváez había acudido a las terapias. Mencionó además que la primera vez ella no la atendió, así que desconoce si es que ella vino con la cédula, pero que la segunda vez, , cuando Wendy sí la había atendido, la procesada había acudido al spa sin la tarjeta de los cupones y sin la cédula, por obvias razones, ya que había comprado el tratamiento con los datos personales del señor Zambrano y con la clave de seguridad de su tarjeta de crédito, pero que la señora hizo escándalo y logró que se la atendiera. Sin embargo, desde ahí, no volvió a venir más al spa:

> WENDY ERIKA VITERI SANCHEZ, Ing. Com. Expresa: Administradora de un spa. - Se le pone a la vista un oficio suscrito por ella, requirieron información y si constaba el nombre de la señora Andrea Lissette Espinoza Narváez, en los archivos, ella canceló por medio de internet, le dijimos que en su segunda sesión le pedidos que traiga su cédula, porque no aparecía su pago la primera vez que fue.- Mi Spa está ubicado arriba de la botica inglesa. Por brindar un buen servicio a los clientes, era un

> tratamiento IPL, que dura seis. Esa tarjeta no me compró a mi sino a Cuponcity, yo no atiendo personalmente tengo como 30 empleados, pero el día que llamó la fiscalía justamente estaba yo. El primer día no había presentado ni cupón ni la cédula, no puedo decir si es ella.

Por otro lado, las únicas pruebas que presentó la defensa de la procesada, era el testimonio de la misma, alegando que ella jamás ha hecho compras de cupones a la plataforma *Cuponcity, cuponazo y cuponera*, y que sí iba al spa, pero que los pagos los realizaba en efectivo, pagando un tratamiento de liposucción de los brazos, pero que le habían dejado mal y por eso dejó de ir. Además, decía que nunca había tratado con el señor Zambrano, sino que solo trabajaba con él en el dispensario de salud y que no tenía amistad con él como para saber el código de seguridad y número de sus tarjetas. De igual manera, menciona que en las Tap (computadoras de acceso para los empleados y trabajadores del dispensario de salud) todo el mundo ingresaba, por lo que no tenían pruebas para acusarla a ella de haber ingresado a realizar la compra.

Sin embargo, todas estas alegaciones son contradictorias con las pruebas documentales y materiales antes señaladas, ya que la misma administradora de *THAI MASSAGE & SPA*, Wendy Erika Viteri Sánchez había mencionado que la vio a la procesada la segunda vez que acudió al spa, a realizarse un tratamiento de IPL (distinto al que alega ella sobre la liposucción), y sin los cupones. Además, la compra de ella estaba registrada en la plataforma de *Cuponcity*, lo cual ella niega en su versión, pero sería desmentido tanto con el testimonio y oficio de la administradora del Spa, como con la pericia informática realizada en las computadoras Tap del centro de salud, en las que se pudo determinar que, contrariamente a lo que ella alega, es desde el usuario de ella mismo desde donde se registra la realización de la compra.

Por tanto, de todo este caso, se infiere que la técnica utilizada por la procesada para apropiarse de los datos financieros de la víctima, fue la del *scanning*, que, como se mencionaba antes, consiste simplemente en mirar el código de seguridad y la información

de la tarjeta de crédito de la víctima, cosa que la procesada pudo hacer cuando el señor Zambrano olvidaba su tarjeta en el dispensario o con los estados de cuenta del señor.

Por esta razón, el juez del Tribunal Único de Garantías Penales del Guayas, dicta la siguiente sentencia:

> ADMINISTRANDO JUSTICIA EN NOMBRE DEL PUEBLO SOBERANO DEL ECUADOR Y POR AUTORIDAD DE LA CONSTITUCION Y LAS LEYES DE LA REPUBLICA, declara a la procesada Andrea Lissette Espinoza Narváez, ecuatoriana, de 28 años, soltera, cosmetóloga, domiciliada en Las Orquídeas, Mz 70 2048, católica, RESPONSABLE, en el grado de AUTORA DIRECTO del delito que tipifica y reprime el artículo Art.190, incisos primero y segundo en concordancia del Art. 42, N° 1, literal a), todos del Código Orgánico Integral Penal, imponiéndole a la pena privativa de libertad de UN AÑO DE PRIVACIÓN DE LIBERTAD y multa de cuatro salarios básicos unificados del trabajador en general, que es la que corresponde al delito según la disposición 6° del artículo 70 ibídem; como reparación integral a la víctima y acusador particulares la cantidad de Dos Mil quinientos Dólares ($2.500,00); además, la pérdida de los derechos de participación, por el tiempo de la pena, como lo dispone el Art. 68 del mismo cuerpo legal.

6.1.3. Percepción de los profesionales del derecho respecto a las implicaciones jurídicas y financieras del delito de apropiación fraudulenta por medios electrónicos

El presente apartado se desarrollará a través del método socio-jurídico, utilizando la técnica de la entrevista, y con el instrumento del cuestionario de preguntas estructuradas. Primero, se colocarán los resultados en una tabla y posteriormente, se los analizará en la discusión.

Entrevistado 1: Dr. Sergio Peralta Armas – Asesor jurídico Banco del Pacifico. 1 año y 7 meses de Experiencia en la institución financiera.

El Dr. Sergio Peralta Armas es abogado con una amplia trayectoria en el ámbito financiero y legal. Actualmente se desempeña como asesor jurídico en el Banco Pacífico, donde ha adquirido una vasta experiencia en el asesoramiento legal relacionado con delitos financieros y fraudes electrónicos. Su perspectiva profesional y conocimiento práctico del sistema bancario en Ecuador lo convierten en una fuente clave para el análisis de la prevención y persecución de delitos de apropiación fraudulenta en el sector financiero.

1.- ¿Cuál es el tiempo que viene desempeñando sus funciones de asesoría jurídica en esta institución financiera?
Transcripción del entrevistado: Actualmente me encuentro desempeñando mis funciones durante un año siete y meses ininterrumpidos en la institución.
2.- ¿En el tiempo que desempeña como asesor(a) jurídico(a) del Banco Pacífico, ¿cuántas incidencias fueron reportadas por los clientes que fueron víctimas de fraude por medios electrónicos?
Transcripción de la respuesta del entrevistado: Desde que desempeño mis funciones aquí en el banco se han reportado cinco incidencias.
3.- ¿La institución financiera para la cual prestó sus servicios, ¿posee algún tipo de protocolos, políticas o programas dirigidos a proteger a sus clientes de este tipo de acciones?
Transcripción de la respuesta del entrevistado: Claro que sí, los protocolos de ciberseguridad son en tres momentos: "Antes, Durante y Después". **a) Antes:** describe a la seguridad del cuentahorrista o tarjetahabiente y es su responsabilidad el uso de los datos y demás **b) Durante:** una vez realizado un consumo no reconocido se envía una aleta a dispositivos de notificaciones. Si no hay respuesta se entiende como positivo

para el banco si existe una incidencia se bloquea la tarjeta y el consumo entra a investigación c) **Después:** se emite resolución de si esos valores son devueltos o no en caso de no ser devueltos puede escalarse a la súper de bancos con el investigador / defensor.
4.- ¿Los clientes que resultaron afectados por la conducta ilícita descrita en el artículo 190 del COIP, ¿recibieron algún tipo de compensación por parte de la institución financiera?
Transcripción de la respuesta del entrevistado: Si el valor torna como no reconocido y se evidencia, el seguro del banco repone esta cantidad.
5.- ¿Desde su experiencia profesional, ¿cómo evalúa la claridad y efectividad de las leyes actuales en la persecución de delitos de apropiación fraudulenta por medios electrónicos?
Transcripción de la respuesta del entrevistado: Existen ocasiones que los bancos niegan la posibilidad de reponer estos valores y por eso se debe acudir a la Superintendencia de bancos.
6.- ¿Cuáles son las principales dificultades jurídicas para la identificación y el enjuiciamiento de los sujetos activos de este tipo penal?
Transcripción de la respuesta del entrevistado: Cuando son de servidores o IP desconocidos y no podemos dar con los autores del delito.
7.- ¿Según su interpretación del tipo penal, ¿qué aspectos clave deben probarse para establecer la comisión del delito de apropiación fraudulenta por medios electrónicos?
Transcripción de la respuesta del entrevistado: **"**1 sujeto activo, 2 sujeto pasivo" En estos casos el sujeto pasivo por su falta de conocimiento es susceptible de caer y ser víctima del delito.

Debemos analizar los medios para la utilización como medio fin del delito de esa forma podemos tener conocimiento más amplio de las formas en la que actúa el activo.
8.- ¿Qué medidas considera esenciales para fortalecer la capacidad del sistema judicial en la prevención y resolución de casos de apropiación fraudulenta por medios electrónicos?
Transcripción de la respuesta del entrevistado: Educación para los clientes de las IF a fin de que tengan mejor manejo de sus tarjetas, cuentas y demás.

Entrevistado 2: Dr. Alex Rubén Benítez Veloz – Cargo: Fiscal. 12 años de experiencia general en el ámbito de Derecho.

El Dr. Alex Rubén Benítez Veloz es fiscal de la Fiscalía General del Estado, con experiencia en la investigación y persecución de delitos relacionados con el fraude electrónico y otros ilícitos financieros. Su conocimiento del proceso penal y su rol como representante del sistema de justicia lo posicionan como un referente clave para analizar las implicaciones jurídicas y los retos asociados al delito de apropiación fraudulenta por medios electrónicos en Ecuador.

1.- ¿Cuál es el tiempo que viene desempeñando sus funciones de asesoría jurídica en esta institución financiera?
Transcripción de la respuesta del entrevistado: Mis funciones las vengo desempeñando desde marzo del 2010 en la FGE, tengo 12 años de experiencia en el campo del derecho.
2.- ¿En el tiempo que desempeña como fiscal, ¿cuántas incidencias fueron reportadas por las instituciones financieras y sus clientes que fueron víctimas de fraude por medios electrónicos?

Transcripción de la respuesta del entrevistado: Se han reportado aproximadamente un valor aproximado de 50 incidencias, tomando en cuenta solo el año 2023 y 23 casos en el año 2024 en la ciudad de Ibarra.
3.- ¿La institución financiera para la cual prestó sus servicios, ¿posee algún tipo de protocolos, políticas o programas dirigidos a proteger a sus clientes de este tipo de acciones?
Transcripción de la respuesta del entrevistado: La Superintendencia de Bancos conjuntamente con el Gobierno Nacional, adoptaron un sin número de medidas, así como políticas públicas y protocolos de ciberseguridad para garantizar los datos de los clientes de las instituciones financieras. Estas instituciones financieras tienen la obligación de contar con un departamento de ciberseguridad, por si se presentan inconvenientes en las transacciones o el sistema financiero, presenta errores.
4.- ¿Los clientes que resultaron afectados por la conducta ilícita descrita en el artículo 190 del COIP, ¿recibieron algún tipo de compensación por parte de la institución financiera?
Transcripción de la respuesta del entrevistado: Más que recibir algún tipo de compensación, en el caso de que exista algún inconveniente en sus transacciones bancarias, así como errores del sistema financiero del banco, dicha institución financiera deberá realizar un estudio y un seguimiento del requerimiento del cliente para determinar si amerita la restitución del valor del cliente. la compensación depende de cada caso y de las políticas internas de la institución afectada. Algunas entidades bancarias y cooperativas han optado por resarcir a los clientes, mientras que en otros casos se ha dejado la responsabilidad a las decisiones judiciales, donde las víctimas deben iniciar acciones civiles o penales para obtener una reparación económica.

5.- ¿Desde su experiencia profesional, ¿cómo evalúa la claridad y efectividad de las leyes actuales en la persecución de delitos de apropiación fraudulenta por medios electrónicos?
Transcripción de la respuesta del entrevistado: A pesar que las instituciones financieras tienen la obligación de garantizar el patrimonio económico transaccional de sus clientes, las instituciones financieras tardan un periodo considerable de tiempo para restituir el bien económico o negar el mismo al cliente, la superintendencia de bancos es el ente rector y regulador de hacer cumplir las leyes.
6.- ¿Cuáles son las principales dificultades jurídicas para la identificación y el enjuiciamiento de los sujetos activos de este tipo penal?
Transcripción de la respuesta del entrevistado: Las principales dificultades incluyen la identificación de los responsables debido al anonimato que permite el entorno digital, la complejidad técnica para rastrear las transacciones electrónicas y la falta de recursos tecnológicos en el sistema judicial. Además, la colaboración internacional en casos donde los delincuentes operan desde el extranjero puede ser lenta y burocrática, complicando aún más el proceso judicial.
7.- ¿Según su interpretación del tipo penal, ¿qué aspectos clave deben probarse para establecer la comisión del delito de apropiación fraudulenta por medios electrónicos?
Transcripción de la respuesta del entrevistado: Él o los sujetos activos del delito, así como los sujetos pasivos. Y otro de los aspectos claves es el análisis de las fuentes que se utilizaron para la consumación del delito, teniendo un panorama más amplio en el modo de actuar de los sujetos involucrados en el delito.
8.- ¿Qué medidas considera esenciales para fortalecer la capacidad del sistema judicial en la prevención y resolución de casos de apropiación fraudulenta por medios electrónicos?
Transcripción de la respuesta del entrevistado: Para fortalecer la capacidad del sistema judicial se recomienda una mejor cooperación y articulación entre las instituciones

financieras y las autoridades judiciales para el intercambio eficaz y seguro de información ante la materialización de los delitos financieros.

6.2. DISCUSIÓN

Dentro de la presente investigación, se ha realizado un análisis del tipo penal y de todos los elementos que lo conforman, como lo son el sujeto activo, el sujeto pasivo, la conducta delictiva y bienes jurídicos lesionados, la pena y los verbos rectores.

Del sujeto activo, se pudo determinar que se trata de uno no calificado, ya que la apropiación fraudulenta por medios electrónicos no es un delito especial propio, sino un delito común, por lo que la persona que delinque, no necesita poseer determinadas características para configurarse la acción.

Sin embargo, es necesario recalcar que la forma en la que el sujeto activo puede llegar a cometer este delito varía de acuerdo a la modalidad. Así, por ejemplo, una persona sin ningún tipo de conocimiento en informática, puede llegar a cometer el ilícito al momento en el que le sustrae a otra persona la tarjeta y obtiene los códigos de seguridad e información privada suficiente como para realizar compras en línea.

También este delito puede llegar a ser cometido por una persona que tiene conocimiento o información sobre la existencia de dispositivos como el *Skimming* o *Shimmer,* los cuáles sustraen información privada de la tarjeta del usuario sin que éste se dé cuenta, y una vez hecho esto, efectúan las compras fraudulentas.

Por último, el delito puede ser cometido por una persona que conozca lo suficiente sobre informática como para crear páginas web fantasmas donde se engañe al usuario ofreciéndole productos a la venta, los cuáles no existen. El usuario coloca su información personal, piensa que realiza la compra, pero solo se obtienen sus datos personales (algo así como una estafa, pero es peor porque se obtiene toda la información de su tarjeta y se la vende al mercado negro).

El sujeto pasivo en este delito es cualquier persona que sea titular de los datos personales que han sido sustraídos para la apropiación de un bien o el provecho económico, por lo que, en este delito, únicamente puede considerarse como víctima a quienes sean los propietarios de estos datos.

Respecto a los bienes jurídicos que lesiona la conducta delictiva, aquí no solo se habla del patrimonio individual de la persona titular de los bienes y el derecho a la protección de datos personales, sino que se vulnera también la fe y confianza de las personas en las transacciones bancarias, lo cual es un bien jurídico colectivo.

En otras palabras, desde el punto de vista sociológico, se vulnera el derecho de las personas a el efecto que tiene esta conducta antijurídica en la colectividad es que los usuarios ya no se sienten seguros de poder realizar las transacciones bancarias o compras por internet, lo cual afecta también a la larga al patrimonio de quienes realizan ventas lícitas en línea, por lo que dicha actividad genera un perjuicio más grave del que se piensa en la sociedad, motivo por el que es necesario implementar una pena privativa de libertad más severa, atendiendo principalmente a lo señalado por la legislación Colombiana.

En este sentido, se sugiere una reforma legal al art. 190 del COIP, que sancione el delito de apropiación fraudulenta por medios electrónicos con una pena privativa de libertad de tres a cinco años, y una pena pecuniaria proporcional al perjuicio causado en la sociedad y el Estado, que trasciende de la afectación personal del titular de los datos personales.

Por otro lado, todos y cada uno de los verbos rectores que son: la utilización fraudulenta (sin consentimiento) de un sistema informático o redes electrónicas, para la obtención de bienes, valores o derechos; o la inutilización de sistemas de alarma o guarda, en el caso de personas jurídicas (instituciones bancarias) que tienen bajo su disposición, los datos personales (por lo que el presente delito puede cometerse también por omisión); están debidamente individualizados y detallados.

Dicho esto, es menester continuar con el análisis de los casos emblemáticos, se pudo evidenciar precisamente las técnicas de *skimming* y *scanning*. Por un lado, un sujeto fue aprehendido en delito flagrante tras haber utilizado un lector falso de tarjetas de crédito (también conocido como dispositivo *skimmer*) mediante el cual, habría realizado la transacción en *Mi Comisariato* del mall Riocentro Sur de Guayaquil.

Atrapar a este sujeto fue sencillo porque realizó la compra en la misma ciudad donde se encontraba la víctima y el correo electrónico le llegó inmediatamente, por lo que acudió con los oficiales de policía al sitio y para su sorpresa, el infractor seguía en el mall.

El segundo en cambio, era un caso en el que se habría utilizado la técnica del *scanning*, pues la señora Lissette Espinoza, habría realizado una compra por internet de cupones por el valor de 2132,83 $ utilizando los datos financieros de la tarjeta de crédito de la víctima, debido a que tuvo acceso a la tarjeta del sujeto en físico porque ambos trabajaban en el mismo sitio.

La forma en la que se había cometido este delito fue con bastante descuido, pues la sentenciada hizo una compra en un spa, utilizando los datos personales del señor, pero se habría acercado al sitio sin la cédula y sin los cupones a pedir que la atiendan en el spa, y todo esto se pudo evidenciar tanto en la declaración de la administradora del spa, como en el oficio entregado por la misma. Además, la compra habría sido hecha desde las computadoras TAP de la institución en donde ambos trabajaban (Ministerio de Salud, dispensario de salud No. 12), hecho que fue corroborado por medio de una pericia informática en la que se reveló que la procesada había ingresado con su propio usuario. Por último, las declaraciones de la procesada eran totalmente contradictorias con las pruebas materiales, ya que ella decía que no conocía al procesado, pero tanto por la declaración del procesado como por el informe de reconocimiento del lugar de los hechos como en la información de la misma institución, se dio a conocer que ella trabajaba con él como secretaria y ayudante de farmacia. Además, ella decía que realizó las compras de forma directa en el spa, pero a través de la misma pericia informática, y de la solicitud de

información a las instituciones y los oficios que dieron éstas de respuesta, se habría obtenido que ella sí había realizado la compra a *Cuponcity*, hecho que a su vez fue concordante con la declaración de la administradora del spa, quien pudo verificar en el sistema que el pago no fue realizado directamente al spa. Además, en el correo electrónico estaba la compra realizada en dicha plataforma, por lo que, a todas luces, la procesada fue culpable de dicho delito.

Nuevamente se puede apreciar que cuando este delito no se comete con suficiente cautela, sino que se realiza la compra en el mismo lugar en el que reside la víctima, y en compras donde se requiere la presencia física del comprador (como es el caso del tratamiento para un spa) sí es mucho más sencillo que se pueda identificar a los responsables.

Ahora bien, tras haber analizado ambos casos, continúa la pregunta de qué hubiera pasado si las compras se hubieran realizado por internet en otros países y desde un navegador capaz de ocultar la dirección IP, o qué hubiera pasado si hubieran vendido la información de este señor a través del mercado negro, ¿cómo se pudiera capturar a los responsables en estos casos?

De ambos casos analizados también se pueden realizar ciertas inferencias generales. Para empezar, la persona que redacta este trabajo investigativo, ha encontrado alrededor de 6 casos que han obtenido sentencia condenatoria de aproximadamente 60 expedientes electrónicos revisados en el sistema SATJE, de los cuáles, 5 de los 6 casos que han obtenido sentencia condenatoria, se ajustaron a procedimiento abreviado porque era muy clara su participación en el delito cometido.

Esto surge a raíz de que las compras realizadas vía internet, fueron realizadas dentro del territorio nacional, y en sí, en la misma ciudad o provincia en la que la víctima vivía. Los pagos fueron realizados con el número de tarjeta y jamás con efectivo, en instituciones donde se emite una factura electrónica que llega justo a tiempo al correo electrónico de los titulares

de la tarjeta, o simplemente, los estados de cuenta de dichas personas no tardaban demasiado en llegar, por lo que se podía saber exactamente el día, la hora, la fecha, el lugar donde se realizó la compra y en muchas ocasiones, quién había realizado la compra.

Sin embargo, cuando las personas que realizan esta actividad ilícita son más juiciosas, lo hacen de forma más metódica, analítica y con más cuidado de no ser capturados, no realizan las compras en la misma localidad en donde vive la víctima, o incluso, no realizan la compra a nivel nacional y contando con su presencia. En muchos casos, simplemente las personas venden la información o datos financieros personales de las víctimas a sujetos en el extranjero, a través de la web profunda, utilizando exploradores o navegadores como Thor, los cuales dificultan o imposibilitan saber el lugar ni la fecha en la que se realiza esta actividad de venta, e incluso las personas que compran los datos personales financieros de otros seres humanos para posteriormente realizar compras fraudulentas, lo hacen con usuarios falsos, también desde navegadores como Thor, y logran así evadir la justicia:

> Los ciberataques y ciberdelitos tienen como característica fundamental el ser difíciles de rastrear. Al ser ataques y delitos que se realizan remotamente, su persecución no puede valerse de procedimientos ordinarios, requiriéndose necesariamente de análisis o peritajes informáticos. Además de su carácter remoto, este tipo de ataques y/o delitos se valen de técnicas para ocultar la locación desde la cual se originan.

> La deep web es un ejemplo de cómo los ciberdelincuentes anonimizan su conexión por internet, navegando por páginas web no indexadas a los motores de búsqueda y evitando los registros o memoria de los buscadores convencionales como Yahoo, Bing, Google, entre otros. Lo anterior, les permite realizar transacciones y demás actividades no autorizadas por ley en el ámbito cibernético. A esto se suma la dark web que consiste en las páginas web que no pueden ser indexadas por motores de búsqueda y para acceder a ellas se necesita software y configuraciones específicas, manteniendo enlaces encriptados entre el usuario y los servidores de internet.

(Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2021, pág. 27)

En otras palabras, es muy difícil que Fiscalía pueda dar con el paradero de los responsables de estas acciones cuando se las ejecuta con más cautela, porque: primero, la víctima suele enterarse después de meses de que le llega un correo electrónico diciendo que se han realizado compras en otros países, con un usuario falso y utilizando sus datos financieros; segundo, cuando se da con la ciudad en la que se realizó la compra y se sabe quién es el usuario que la realizó, pero el usuario es falso y realizó la compra con el navegador Thor, es muy difícil saber la localización exacta.

Por ejemplo, puede que en su correo electrónico aparezca que usted realizó la compra de un televisor en Londres, con sus datos personales. La compra llega a una locación que realmente no es la del infractor. El sujeto recibe la compra y la llena utilizando sus datos personales y, si es que no le piden cédula, será extremadamente difícil dar con el paradero del mismo. Peor aún, si el sujeto posee documentos falsos, será aún más difícil encontrarlo, y este perfectamente puede ser el estereotipo de quienes hayan logrado, con éxito, cometer esta infracción más de una vez, utilizando conocimientos en informática.

Además, la inferencia anterior, tiene también cierto sustento estadístico. Si bien es cierto que este delito no parece ser denunciado con tanta frecuencia, ya que los informes anuales de gestión de Fiscalía y de rendición anual de cuentas de Fiscalía a nivel nacional, no colocan estos delitos en la lista de los 10 delitos más denunciados, se puede hacer un pequeño análisis manual.

Quien redacta esta investigación, para poder recabar los dos casos analizados, primero ingreso al actual Sistema Automático de Trámite Judicial Ecuatoriano (en adelante, sistema SATJE), y en la parte de consulta de causas, colocó el nombre del tipo penal: Apropiación Fraudulenta por Medios Electrónicos, y se desplegaron información sobre 6311 expedientes

(ver ilustración 1), que eran mostrados de 100 en 100 en cada página de la plataforma (64 páginas de 100 expedientes cada una).

Ilustración 1: 6311 causas de apropiación fraudulenta por medios electrónicos desde el 2014 a la actualidad

Estos casos se recopilan desde la vigencia del COIP (2014) hasta la actualidad, siendo así que se alcanzó a revisar únicamente 7 hojas de 100 (700 expedientes) de los cuáles, hubo únicamente 6 sentencias condenatorias (lo cual se obtuvo mediante búsqueda automática por comandos de nombres con palabras clave) y 7 absolutoria. De las condenatorias, 5 fueron por procedimiento abreviado, y una sola, fue por procedimiento ordinario.

70 causas de 6311 es apenas el 1.10%, y de ese 1.10%, apenas un 8.57% (6 causas de 70) tuvieron sentencia condenatoria, mientras que el 91, 43% de los casos, los expedientes se archivan, y las razones para ello, de acuerdo al artículo 586 del COIP, son las siguientes:

> Art. 586.- Archivo. - Transcurridos los plazos señalados, de no contar con los elementos necesarios para formular cargos, la o el fiscal, en el plazo de diez días, solicitará el archivo del caso, sin perjuicio de solicitar su reapertura cuando aparezcan

> nuevos elementos siempre que no esté prescrita la acción. La o el fiscal solicitará a la o al juzgador el archivo de la investigación cuando:
>
> 1. Excedido los plazos señalados para la investigación, no se ha obtenido elementos suficientes para la formulación de cargos.
>
> 2. El hecho investigado no constituye delito.
>
> 3. Existe algún obstáculo legal insubsanable para el inicio del proceso.
>
> 4. Las demás que establezcan las disposiciones de este Código. (Asamblea Nacional, 2014)

Por tanto, si se sabe que la mayoría de causas que se investigan en Fiscalía por este delito no tienen sentencia condenatoria, se puede inferir que una de las posibles causas es la falta de elementos de convicción, y esto puede deberse, en gran medida (de entre algunas posibilidades), a que existen obstáculos muy relevantes para la investigación y la obtención de elementos de convicción que Fiscalía utilice para demostrar la existencia material de la infracción y la responsabilidad de la persona procesada cuando quienes cometen estos delitos son más meticulosos y metódicos, o realizan compras en el extranjero por internet, o son personas que pertenecen a otra jurisdicción, en cuyo caso, depende de los convenios de Derecho Internacional Privado que existan para sancionar a estas personas.

> Un mayor uso de la Internet implica un aumento en la vulnerabilidad de la ciudadanía que hace uso de esta herramienta, tanto en lo profesional como en lo cotidiano. El aprovechamiento de estas vulnerabilidades en el ciberespacio por parte de actores delictuales se ha convertido en una nueva forma de atentar contra los derechos de las personas.

> Los delitos informáticos son desterritorializados, es decir que no necesariamente se anclan a las naciones, teniendo capacidades transfronterizas que limitan el actuar policial basado en la circunscripción territorial. Este tipo de delito pasa

> completamente desapercibido para la víctima quien, por lo general, no es consciente de haber sido perjudicada. Lo que conlleva que la mayoría de veces quienes han sido afectados, no presenten la debida denuncia ante las autoridades. (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2021, pág. 24)

Doctrinariamente, existen tres teorías respecto a la aplicación de la jurisdicción penal en cuanto al criterio del territorio: la teoría de la actividad, la teoría del resultado, y la teoría de la ubicuidad:

> […] para la teoría de la actividad, el delito se ha cometido allí donde el autor ha realizado su acción, mientras que, para la teoría del resultado, el lugar donde éste se produce es aquél en el que debe considerarse cometido el delito […]
>
> Para la teoría de la ubicuidad, puede considerarse cometido el hecho tanto en el lugar donde se ha llevado a cabo la acción como en aquél en el que se ha producido el resultado" (Conde, 2010, pág. 155 y 156).

El Tratado Internacional de Montevideo de Derecho Penal de 1940, en su artículo 2, se acoge más a la teoría del resultado, pero no este tratado no está ratificado por Ecuador:

> Artículo 2
>
> En los delitos que afecten a dos o más Estados, cometidos por uno o varios delincuentes, serán competentes los jueces o tribunales del lugar en donde hayan sido consumados debiendo aplicarse en el respectivo proceso las leyes locales. Si el delito se hubiere consumado en más de un país, serán competentes los tribunales y se aplicarán las leyes del Estado que hubiere tomado conocimiento judicial en primer término. (Segundo Congreso Suramericano de Derecho Internacional Privado, 1940)

Sin embargo, en este caso, si a una persona le roban información sobre sus datos personales financieros mediante la utilización de lectores de tarjetas falsos con escaneo de códigos CVC (por ejemplo, la clave de seguridad de la tarjeta de crédito, la información de la tarjeta y cédula) y esa información la venden en el mercado negro, desde el momento en el que logran sustraer dicha información, ya hay una vulneración del derecho a la protección de datos personales, a la intimidad y se pone en peligro el patrimonio de la persona, pero dicha vulneración continúa incluso cuando hay alguien en el extranjero que compre esos datos financieros, y si ese alguien realiza una compra, ya se vulnera el patrimonio de la persona, por lo que el delito se consuma tanto en el país donde se sustraen los datos personales como en el país donde se realiza la compra fraudulenta, razón por la que debería aplicarse la teoría de la ubicuidad, además de que esta responde a la necesidad de crear normas internacionales aplicables para casos donde el resultado se produce en ambos países.

Esto sería concordante con el artículo 400, numerales 3 y 4 del Código Orgánico Integral Penal:

> Art. 400.- Ámbito de la potestad jurisdiccional. - Están sujetos a la jurisdicción penal del Ecuador:
>
> […]
>
> 3. Las y los ecuatorianos o las o los extranjeros que cometen una infracción a bordo de naves aéreas o marítimas de bandera ecuatoriana registradas en el Ecuador, ya sea en el espacio aéreo nacional o mar territorial ecuatoriano o en el espacio aéreo o mar territorial de otro Estado.
>
> 4. Las y los ecuatorianos o las o los extranjeros que cometen infracciones contra el derecho internacional o los derechos previstos en convenios o tratados internacionales vigentes, siempre que no hayan sido juzgados en otro Estado. (Asamblea Nacional, 2014)

A su vez, esta disposición del Código sería también respaldada por el Convenio de Derecho Internacional Sánchez y Bustamante, ratificado por Ecuador en el 25 de noviembre del año 2005, mediante registro oficial No. 153:

> Art. 302.- Cuando los actos de que se componga un delito, se realicen en Estados contratantes diversos, cada Estado puede castigar el acto realizado en su país, si constituye por si solo un hecho punible. De lo contrario, se dará preferencia al derecho de la soberanía local en que el delito se haya consumado. (Código de Bustamante, 1928)

Esto significa que debería existir un convenio de cooperación jurídico-penal entre los dos países en los que ocurriría la infracción, lo cual no siempre sucede, y si sucede, el proceso suele demorarse por las diligencias y obstáculos procesales que se suscitan, ya que puede demorar meses o incluso años, el poder sustentar la existencia material de la infracción y la responsabilidad de la persona procesada, o llevar a cabo un juicio y tener una sentencia o resolución.

Además, si a esto se le suma que de acuerdo al artículo 412 del Código Orgánico Integral Penal, el principio de oportunidad puede ser aplicable en los delitos cuya pena privativa de libertad es hasta cinco años, el panorama resulta aún más complicado:

> Art. 412.- Principio de oportunidad. - La o el fiscal podrá abstenerse de iniciar la investigación penal o desistir de la ya iniciada, en los siguientes casos:
>
> 1. Cuando se trate de una infracción sancionada con pena privativa de libertad de hasta cinco años, con excepción de las infracciones que comprometen gravemente el interés público y no vulneren a los intereses del Estado.
>
> 2. En aquellas infracciones culposas en las que el investigado o procesado sufre un daño físico grave que le imposibilite llevar una vida normal.

> La o el fiscal no podrá abstenerse de iniciar la investigación penal en los casos de delitos por graves violaciones a los derechos humanos y delitos contra el derecho internacional humanitario, delitos contra la integridad sexual y reproductiva, delincuencia organizada, violencia contra la mujer o miembros del núcleo familiar, trata de personas, tráfico de migrantes, delitos de odio, de sustancias catalogadas sujetas a fiscalización y delitos contra la estructura del Estado constitucional de derechos y justicia. (Asamblea Nacional, 2014)

Es decir, que la ley penal ecuatoriana faculta a los fiscales la aplicación del principio de oportunidad también para el caso del delito de apropiación fraudulenta por medios electrónicos, lo cual implica el desistir de la investigación de este delito al no encontrar rápidamente elementos de convicción y tener otras causas más importantes o con más probabilidades de ser resueltas que las que implican este delito, considerando que Ecuador aún no ha ratificado el Consejo de Europa (2001).

Por último, si a esto se le añade que, a través de la Resolución No 34-FGE-2023, emitida por la fiscal Diana Salazar, se establece que la Unidad Fiscal especializada en Ciber Delitos tendrá una sola sede, el problema se complica aún más:

> Artículo 1.- Crear la Unidad Nacional Especializada en Investigación de Ciberdelito, […]
>
> Esta unidad tendrá su sede única en la ciudad de Quito, y un ámbito investigativo a nivel nacional, pudiendo a futuro, sobre la base de los informes técnico, jurídico y estadístico, extenderse a otras provincias conforme necesidad institucional. (Fiscalía General del Estado, 2022)

Para tener una idea, hay que considerar que solo desde el año 2020 al 2022, se registraron más de 3000 delitos informáticos, por lo que es reiterada la pregunta de si la única sede de Ciber Delitos puede llegar a resolver todos estos casos, considerando, además, las

estadísticas antes mencionadas sobre el disminuido número de casos que obtienen sentencias condenatorias de la totalidad disponible en el sistema SATJE:

> Los ataques perpetrados por ciber mafias son frecuentes en el país. Según un informe de la Unidad de Ciberdelitos de la Policía, entre 2020 y el 6 de julio de 2022 se registraron 3,183 delitos informáticos. En 2020 se reportaron 682 casos, en 2021 la cifra aumentó a 1,851, y en los primeros seis meses de 2022 ya se han iniciado 650 investigaciones a nivel nacional.
>
> Las provincias con mayor incidencia de estos delitos son Guayas, Pichincha, Manabí, Imbabura, Carchi y Azuay.
>
> Gonzalo García, responsable de la Unidad de Ciberdelitos, señala que el incremento de estos delitos está relacionado con el mayor acceso de la población a Internet y a las redes sociales. Datos oficiales indican que el 79.21% de los ecuatorianos tiene acceso a la web y aproximadamente 15.8 millones de personas en el país poseen cuentas en diversas plataformas sociales.
>
> Un informe de la Interpol (Policía Internacional) también menciona que "[…] Los delincuentes están aprovechando esa transformación en línea para atacar, a través de las redes y sistemas informáticos". (El Comercio, 2022)

Por tanto, con 3183 casos de delitos informáticos, para un fiscal coordinador de asuntos administrativos y algunos agentes fiscales (en la resolución, no se menciona el número) habría que preguntarse si existe suficiente personal como para llevar a cabo la investigación de todas estas denuncias por delitos informáticos, y la respuesta parece estar justamente en las cifras antes mencionadas dentro del sistema SATJE, que establecerían que solo el 6 de 70 causas llegan a sentencia condenatoria, mientras que la mayoría de causas son archivadas, y muchas de ellas, como se mencionaba anteriormente, por falta de elementos de convicción suficientes. La inferencia de ello, es que Ecuador no se encuentra aún preparado para poder lidiar con los desafíos de ciberseguridad y la lucha contra los delitos informáticos de la mejor manera posible. De hecho, existen estudios que confirman que el nivel de vulnerabilidad ante estos delitos, es alto:

> Según el Índice Global de Ciberseguridad (GCI) publicado por la ITU el 9 de julio de 2019, Ecuador es un país vulnerable a las amenazas cibernéticas, ubicándose en el lugar 98 de 193 países, siendo el número 193 el que presenta mayor vulnerabilidad a nivel mundial. Además, de acuerdo con datos de Kaspersky Lab (2020) sobre ataques cibernéticos dirigidos a Ecuador, el país se posiciona en el puesto 89 dentro del ranking mundial de naciones más atacadas (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2021, p. 28).

Y en especial, la mayor vulnerabilidad a la ciberseguridad o el delito informático con mayor incidencia en Ecuador, desde el año 2018 al 2020, según el Ministerio de Gobierno, es la apropiación fraudulenta de medios electrónicos:

> La información que mantiene el Ministerio de Gobierno evidencia que el principal delito informático que afecta a la población es la apropiación fraudulenta por medios electrónicos. La siguiente tabla muestra el listado de delitos informáticos registrados en los años 2018, 2019 y 2020. (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2021, pág. 25)

Ahora bien, este acápite no puede finalizar sin antes incorporar la percepción de los profesionales del Derecho respecto a esta materia. Primero, respecto a las preguntas1 y 2, Sergio Peralta Armas, Ab. Del Banco del Pacífico, señala que viene desempeñando sus funciones en asesoría jurídica durante 7 meses, y que, durante ese tiempo, los clientes de la institución financiera han reportado 5 incidentes de fraude por medios electrónicos (preguntas 1 y 2).

Por otro lado, el segundo entrevistado, señala que ha venido trabajando en Fiscalía desde hace 12 años atrás. También ha manifestado que durante este tiempo que lleva trabajando para la institución, se han reportado 25 incidencias en el año 2024 y 50 en el 2023.

Ahora bien, en referencia a los protocolos de seguridad que existen para prevenir o combatir esta forma de delincuencia, Sergio manifiesta que existen protocolos de actuación por parte de la institución financiera en 3 momentos: antes, durante, y después

- Antes: describe a la seguridad del cuentahorrista o tarjetahabiente y es su responsabilidad el uso de los datos y demás.
- Durante: una vez realizado un consumo no reconocido se envía una alerta a dispositivos de notificaciones. Si no hay respuesta se entiende como positivo para el banco si existe una incidencia se bloquea la tarjeta y el consumo entra a investigación
- Después: se emite resolución de si esos valores son devueltos o no; y en caso de no ser devueltos, puede escalarse a la súper de bancos con el investigador / defensor.

Por otro lado, el señor Fiscal señala que las instituciones bancarias deben contar con protocolos de ciberseguridad para prevenir la comisión de estos delitos, y señala también que existen políticas públicas relacionadas a prevenir la comisión de los mismos.

Lamentablemente, estos protocolos no cubren ciertas cuestiones como el hecho de no saber o no poder manejar correos electrónicos de forma constante como para recibir las alertas de consumo o compras realizadas con la tarjeta de crédito o débito. Esto principalmente les puede suceder a las personas mayores o a adolescentes que ya poseen tarjetas de crédito o débito.

Además, no es cierto que a todos los usuarios que van a tener una tarjeta, se les informa sobre este particular, ya que muchas veces se asume que esto es de conocimiento público. Los bancos no suelen informar ni sobre el cuidado físico que hay que tener con respecto a los códigos de tarjetas de crédito o débito, ni mucho menos sobre la existencia de los dispositivos *skimming* o *shimmer*. De igual manera, a los usuarios no se les menciona respecto al *fishing* con páginas fraudulentas o páginas que roban información (lo cual es sumamente necesario, en especial para adolescentes), ya que esto se asume como responsabilidad del mismo titular de la tarjeta o de la cuenta bancaria.

Aquí es menester mencionar que desde el punto de vista jurídico y de acuerdo con la teoría de Ghunter Jakobs (1997) sobre imputación objetiva, las personas al no ejercer un rol profesional específico, tienen solo el rol del ciudadano común, lo cual implica únicamente no vulnerar el derecho ajeno, pero al no ser profesionales capacitados y encargados de la vigilancia y protección de datos personales de los individuos, no se les puede exigir que estén capacitados sobre esta materia (pese a ser titulares de sus datos personales, porque quien está encargado de protegerlos es la institución bancaria que cumple el rol de su vigilancia), entonces aquí no hay imputación a la víctima por no ejercer el deber objetivo de cuidado.

Sin embargo, por lógica es necesario que los usuarios sepan cuál es la forma en la que se protege sus datos personales, capacitándose con la protección de los mismos y la manera en cómo se cometen estos delitos, pero aquí sí es importante que las instituciones bancarias no solo informen a los titulares de las cuentas respecto a no dar los datos personales ni realizar compras fraudulentas, sino una información más profunda (incluyendo información respecto a los mencionados dispositivos de comisión). En síntesis, se debería de capacitar al usuario con el contenido del primer objetivo de este trabajo de titulación, respecto a todas las formas de comisión de este tipo penal.

Los valores suelen ser devueltos por parte de la institución bancaria únicamente bajo resolución de la Superintendencia de Bancos, dado que eso deviene en la función que tienen las aseguradoras de los bancos, pero no le sería imputable a la institución bancaria a menos que la misma haya omitido enviar la alerta por correo electrónico al usuario, aunque esta alerta no debería de ser la única (por ejemplo, debería enviarse alerta también por mensaje de texto al teléfono móvil).

Precisamente por ello, se le pregunta a Sergio si los clientes reciben algún tipo de compensación por el valor sustraído por apropiación fraudulenta de medios electrónicos si

es que el valor torna como no reconocido y se evidencia, el seguro del banco repone esta cantidad.

Además, Sergio señala que, en algunos casos, los bancos niegan la posibilidad de reponer esos valores, por lo que deben acudir a la superintendencia para hacerlo, siendo concordante con lo señalado anteriormente, lo cual evidencia que no existe claridad, sino que debe ser la entidad pública rectora en cuestiones bancarias, la que lo debe determinar. Esto además es concordante también con la respuesta señalada por el señor Fiscal, quien reitera que sí existe cierta responsabilidad por parte de las instituciones bancarias en estas situaciones.

A continuación, se les pregunta cuáles son las principales dificultades para el enjuiciamiento de estos delitos y el Abogado responde que se presenta dificultad únicamente en los casos en los que se desconoce el servidor IP, lo cual es extremadamente sencillo de hacer hoy en día, a través de navegadores como Thor, mismos que son de fácil acceso, descarga y utilización del público en general.

Algo similar señala el segundo entrevistado, quien menciona que lo complicado en este tipo de casos es obtener las pruebas que evidencien la responsabilidad de la persona que ha cometido el delito.

De igual manera, cuando se le pregunta cuáles son los elementos necesarios para probar estos delitos, el abogado responde que hay que probar tres: sujeto activo, pasivo y medios. Aquí hay que destacar que, uniendo lo dicho anteriormente, lo complicado viene a ser probar el sujeto activo, dado que éste se oculta a través del bloqueo de su dirección IP en los navegadores antes mencionados, cosa que también es concordante con lo manifestado por el señor fiscal, ya que menciona que la dificultad se encuentra en identificar fuentes o redes donde se perpetró el ilícito, precisamente en aquellos casos donde se oculta la dirección IP.

Finalmente, cuando se le pregunta al Doctor cuáles son las medidas que considera idóneas desde el punto de vista legal para fortalecer la seguridad contra la comisión de este delito, Sergio señala que lo más idóneo es capacitar al usuario en materia de seguridad digital y que tengan mejor manejo de su tarjeta, cuenta, etc.

En cambio, a esta pregunta, el segundo entrevistado señala que lo más importante y necesario es la cooperación y articulación entre las instituciones financieras y las autoridades judiciales para el intercambio eficaz y seguro de información ante la materialización de los delitos financieros.

Ciertamente ambas posturas son idóneas y resultarían útiles para alertar al usuario sobre la posibilidad de que se cometan estos ilícitos, y definitivamente, disminuirían la incidencia del fraude electrónico en el Ecuador, pero también es necesario que la pena prevista para el tipo penal sea proporcional al perjuicio ocasionado al individuo, a la sociedad y al Estado.

7. CONCLUSIONES

a) El delito de apropiación fraudulenta por medios electrónicos, tipificado en el Código Orgánico Integral Penal (COIP), se caracteriza por la utilización de herramientas tecnológicas para acceder ilícitamente a bienes económicos ajenos, vulnerando el derecho a la propiedad y generando un impacto negativo en las víctimas y en la confianza en el sistema financiero. Entre los elementos esenciales de este tipo penal destacan el uso indebido de plataformas electrónicas y la intención dolosa del autor, aspectos que, aunque bien definidos en la normativa, presentan desafíos significativos en su aplicación práctica. Asimismo, se concluyó que el marco jurídico actual puede ser complementado mediante la incorporación de lineamientos claros sobre la responsabilidad de las entidades financieras en la prevención de fraudes electrónicos y el diseño de protocolos tecnológicos más robustos. Esto, sumado a la implementación de herramientas tecnológicas avanzadas, permitiría no solo sancionar con mayor eficacia este delito, sino también prevenir su ocurrencia, brindando mayor protección al bien jurídico tutelado.

b) Se identificó y describió los elementos del tipo penal de la apropiación fraudulenta por medios electrónicos, establecido en el artículo 190 del Código Orgánico Integral Penal, concluyendo en lo principal que se debe implementar una reforma al mencionado artículo, estableciendo que la pena debe ser más proporcional a la infracción cometida, por lo que se sugiere una pena más severa de tres a cinco años de privación de libertad; y una pena pecuniaria de 100 a 1000 salarios básicos unificados del trabajador en general.

c) Del análisis de ambos casos analizados, se realizaron algunas inferencias inductivas de gran relevancia: primero, recabar elementos de convicción para probar la existencia material de la infracción y la responsabilidad de la persona procesada en estos delitos es más sencillo cuando el sujeto activo realiza las compras fraudulentas con sus propios datos personales y en la misma localidad o provincia en la que reside la víctima, porque las pruebas se obtienen de los hechos narrados por los sujetos

procesales, que tienen que ser corroboradas con los oficios de las instituciones involucradas en la transacción respecto a los hechos ocurridos; segundo, en el proceso de búsqueda de casos que puedas ser analizados en este trabajo investigativo, se determinó que colocando el delito en el buscador del sistema SATJE, salen la mayor parte de causas registradas, que correspondían a la información de 3611 expedientes aproximadamente, dividida en 64 páginas que desplegaban 100 expedientes cada una, de las cuáles se revisó 7 páginas (información de aproximadamente 700 expedientes) , obteniendo únicamente 6 sentencias condenatorias, y 7 absolutorias. Es decir, de cada 700 expedientes, 13 llegan a sentencias, de lo que se deriva que la mayoría de los casos no llegan a sentencia y se archivan; tercero, si se entiende que es más fácil para Fiscalía investigar los delitos de apropiación fraudulenta cuando los sujetos que roban información financiera de los usuarios, son los mismos que realizan las compras con sus propios datos personales y en el mismo sitio en el que viven sus víctimas, y a su vez, se sabe que la mayoría de los casos no llegan a sentencia, se puede inferir que la mayoría de estos delitos no se cometen por esta modalidad, sino por la venta de información financiera de los usuarios a personas en el extranjero, por venta de tarjetas clonadas, entre otras que dificultan la investigación de fiscalía (la mayoría de la los infractores, sí son meticulosos al momento de cometer la infracción); cuarto, 5 de 6 sentencias condenatorias fueron por procedimiento abreviado, lo que significa que el Fiscalía solo alcanza a recabar elementos de convicción suficientes en los casos en la minoría de los casos, y esto se puede deber a que la mayoría de personas que cometen este delito, lo hacen tomando precauciones mediante la utilización de navegadores que ocultan la dirección IP, o por medio de la venta de información a personas en el extranjero (y ocultando su verdadera identidad a los compradores en el mercado negro), lo cual les disminuye considerablemente el riesgo de ser capturados; quinto, esto implica que Fiscalía, al realizar la investigación de estos delitos, se encuentra con muchas dificultades, como son: la necesidad de que ambos países estén sujetos a convenios de Derecho Internacional privado en los que se establezca la cooperación penal y se resuelvan los conflictos de jurisdicción y competencia cuando el resultado dañoso se ha producido en ambos Estados, la necesidad de investigar una cadena de sucesos en los que los infractores han protegido meticulosamente su identidad y su

lugar de residencia o han permanecido en el anonimato ya que toda la operación se pudo haber llevado a cabo en la web profunda, la falta de registro suficiente de datos de los infractores por parte de las entidades involucradas al momento de realizar la compra, el tiempo transcurrido entre el robo de información y el momento en el que la víctima se entera del robo, el poder descifrar direcciones IP encriptadas; sexto, la falta de sedes de Unidades Fiscales Especializadas en Ciberdelitos es una causa más para que muchos casos se queden en el archivo y no lleguen a obtener una sentencia, debido a que los pocos fiscales que se encuentran en dicha unidad, tienen tantos casos que no se dan abasto y le deben dar prioridad solo a los casos en los que hay mayor probabilidad de encontrar una resolución (que son los casos donde los delincuentes fueron mucho menos meticulosos y realizaron las compras a su nombre y en el mismo lugar donde residía la víctima, como los analizados en esta investigación).

d) La finalidad de las entrevistas fue evaluar las implicaciones jurídicas y financieras del delito de apropiación fraudulenta por medios electrónicos, basándose en la opinión de expertos en el área financiera. se planificó entrevistar tanto al Dr. Sergio Peralta Armas, asesor jurídico del Banco del Pacífico, como al Dr. Alex Rubén Benítez Veloz, fiscal de la FGE, la dificultad para acceder a ambos especialistas llevó a priorizar el criterio del Dr. Benítez.

   El fiscal señaló que este delito plantea desafíos significativos en su investigación y sanción, como la identificación de los autores y el rastreo de los fondos. Si bien el COIP establece un marco jurídico adecuado, se identifican carencias en la capacitación técnica y la coordinación entre las instituciones bancarias y judiciales. Estos factores afectan tanto la efectividad de la persecución penal como la confianza en el sistema financiero. En síntesis, la lucha contra este tipo de delitos exige no solo un marco normativo robusto, sino también un enfoque integral que fortalezca la cooperación interinstitucional, la ciberseguridad y la prevención de fraudes electrónicos.

8. RECOMENDACIONES

a) Incrementar el número de sedes de la Unidad Fiscal Especializada en Ciberdelitos creada en el año 2021, ya que solo existe una sede en Quito. Especialmente, debe considerarse implementarlas en: Guayas, Pichincha, Manabí, Imbabura, Carchi y Azuay, que, según los reportes de la prensa, son las provincias con mayor incidencia en estos delitos. Esto en virtud de que la tendencia ha ido en aumento respecto a los delitos informáticos, y en especial, al delito de apropiación fraudulenta de medios electrónicos (entre el año 2020 a julio de 2022, ya se registraban 3183 casos; y en el sistema SATJE, del año 2014 hasta la actualidad, se arroja información aproximada de más de 6000 expedientes). En sí, la falta de sedes vendría a ser una causa más para que la mayoría de estos expedientes sean archivados y no lleguen a sentencia, pues en virtud del principio de oportunidad, Fiscalía puede considerar que existen casos con mayor probabilidad de ser solucionados que otros, por lo que muchos casos se quedan en el archivo por falta de recursos humanos suficientes para realizar la investigación previa.

b) Implementar campañas de socialización en todas las instituciones de educación superior del Ecuador respecto al cuidado y protección de los datos personales financieros y utilización responsable de las redes sociales, a fin de que exista cada vez más consciencia respecto a los riesgos de realizar compas en páginas web que no son seguras, a entregar información financiera a sitios que no son confiables, a descuidar tarjetas u otros objetos personales en sitios donde hay personas que puedan robar la información de los usuarios, entre otras cuestiones.

c) Establecer leyes, reglamentos y medidas administrativas que impongan la obligación de las instituciones bancarias de informar a los usuarios respecto a los mecanismos de seguridad que existen para proteger sus datos financieros personales, así como los riesgos que existen de que puedan robar dichos datos, y las modalidades que existen de robo de dichos datos personales por medios electrónicos.

d) Utilizar responsablemente las redes sociales, sin brindar mayor información que la necesaria; y evitar realizar compras en sitios web de los que no se tenga mucha información o que no sean lo suficientemente confiables para el usuario, así como evitar dar información financiera personal a ningún individuo sin conocerlo; y evitar olvidar pertenencias que contengan información sobre datos personales en ningún lugar.

9. REFERENCIAS BIBLIOGRÁFICAS:

Andrade, M. Y. (2015). *La víctima en el Código Orgánico Integral Penal*. Obtenido de VLEX: https://vlex.ec/vid/victima-codigo-organico-integral-682467049

Asamblea Constituyente. (2008). *Constitución de la República del Ecuador.* Montecristi: Registro Oficial No. 449.

Asamblea Legislativa de la república de Costa Rica . (10 de Julio de 2012). *Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal*. Obtenido de N° 9048: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?param1=NRTC&nValor1=1&nValor2=73583&nValor3=90354&strTipM=TC#:~:text=Suplantación%20de%20identidad-,Será%20sancionado%20con%20pena%20de%20prisión%20de%20tres%20a%20seis,cause%2

Asamblea Legislativa de la República de el Salvador. (26 de Febrero de 2016). *Ley especial contra los delitos informáticos y conexos*. Obtenido de DECRETO N° 260: https://www.fiscalia.gob.sv/medios/portal-transparencia/normativas/normativas-de-interes/ley-especial-contra-delitos-ciberneticos.pdf

Asamblea Nacional . (2014). *Código Orgánico Integral Penal.* Quito: Registro Oficial No. 180.

Asamblea Nacional. (15 de Febrero de 2012). *Código Penal* . Obtenido de Registro Oficial Suplemento 147 de 22-ene-1971: https://www.oas.org/juridico/pdfs/mesicic4_ecu_penal.pdf

Banco Compartamos. (5 de mayo de 2023). *¿Qué es el skimming y scanning? ¡Protege tus datos bancarios!* Obtenido de Banco Compartamos: https://www.compartamos.com.mx/compartamos/blog/cuida-tu-cartera/que-es-el-skimming-y-scanning#:~:text=Tanto%20el%20skimming%20como%20scanning,informaci%C3%B3n%20de%20las%20tarjetas%20bancarias.

BBVA . (2023). *¿Qué es el CVV o CVC de las tarjetas de crédito?* Obtenido de BBVA : https://www.bbva.com/es/salud-financiera/que-es-el-ccv-o-cvc-en-las-tarjetas-de-credito/

Benavides, M. M., Acosta, M. G., & García, N. P. (2020). *Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios*. Revista Venezolana de Gerencia, vol. 25, núm. 89, 351-368.

Carrillo, M. R. (2013). *Los desafíos del derecho penal frente a los delitos informáticos y otras conductas fraudulentas en los medios informáticos.* IUS. Revista del Instituto de Ciencias Jurídicas de Puebla A.C., vol. VII, núm. 31, 207-222.

Caso Gaibor, *apropiación fraudulenta por medios electrónicos*, 09281201802880 (Unidad Judicial con Competencia en Delitos Flagrantes 29 de junio de 2018).

Caso Zambrano, *apropiación fraudulenta por medios electrónicos*, 09284201701374 (Tribunal Único de Garantías Penales del Guayas 28 de marzo de 2019).

Código de Bustamante. (20 de Febrero de 1928). *Convenio de Derecho Internacional Privado Sánchez de Bustamante*. Obtenido de Código de erecho Internacional Privado : https://www.oas.org/juridico/spanish/mesicic3_ven_anexo3.pdf

Conde, F. M. (2010). *Derecho Penal, Parte General.* Madrid, España: Tyrant lo Branch.

Congreso de Colombia . (24 de Julio de 2000). *Código Penal Colombiano*. Obtenido de Ley 599 de 2000 (Actualizado en 2023. Diario Oficial No. 44.097: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=6388

Consejo de Europa. (2001). *Convenio sobre la ciberdelincuencia.* Budapest, Hungría: Serie de Tratados Europeos No 185. Obtenido de http://www.noalacosovirtual.pe/convenio-budapest-ciberdelincuencia.PDF

El Comercio. (25 de julio de 2022). *3 183 delitos informáticos se han registrado en el Ecuador, desde el 2020*. Obtenido de El Comercio: https://www.elcomercio.com/actualidad/seguridad/3183-delitos-informaticos-se-han-registrado-en-el-ecuador-desde-el-2020.html

Enríquez, L. (31 de Agosto de 2022). *Hacia una cultura de "Valor al Riesgo" en la ciberseguridad del Ecuador*. Obtenido de Universidad Andina Simón Bolívar: https://www.uasb.edu.ec/ciberderechos/2022/08/31/hacia-una-cultura-de-valor-al-riesgo-en-la-ciberseguridad-del-ecuador/

Fiscalía General del Estado. (13 de junio de 2015). *Los delitos informáticos van desde el fraude hasta el espionaje*. Obtenido de Fiscalía General del Estado: https://www.fiscalia.gob.ec/los-delitos-informaticos-van-desde-el-fraude-hasta-el-espionaje/

Fiscalía General del Estado. (2022). *Resolución No. 34-FGE-2022.* Quito: Fiscalía General del Estado.

Galeas, L. D. (Diciembre de 2022). *Análisis y simulacion de un ataque de Phishing en el uso de un Framework Gophish en la Cooperaiva de Taxis "San Fernando de Babahoyo".* Obtenido de Universidad Técnica de Babahoyo: http://dspace.utb.edu.ec/handle/49000/11697

Harán, J. M. (14 de Octubre de 2021). *Banco Pichincha sufrió ataque informático que afectó parte de sus servicios*. Obtenido de WeliveSecurity: https://www.welivesecurity.com/la-es/2021/10/14/banco-pichincha-sufrio-ataque-informatico/

Kaspery Security. (7 de octubre de 2023). *Qué es una dirección IP: definición y explicación*. Obtenido de Kaspery Security: https://latam.kaspersky.com/resource-center/definitions/what-is-an-ip-address

LP. Pasión por el Derecho. (20 de septiembre de 2021). *¿Cuáles son las clases de tipos penales? Bien explicado*. Obtenido de LP. Pasión por el Derecho: https://lpderecho.pe/cuales-son-las-clases-de-tipos-penales-bien-explicado/

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2021). *ACUERDO MINISTERIAL 006-2021*. Obtenido de https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Acuerdo-No.-006-2021-Politica-de-Ciberseguridad.pdf

Pintado, A. G. (2019). *Análisis Jurídico de las leyes que amparan a víctimas de delito informatico en Santo Domingo* . Santo Domingo, Ecuador: Universidad Regional Autónoma de los Andes "UNIANDES".

PUCE. (18 de diciembre de 2017). *Dominios Académicos y líneas de investigación.* Obtenido de Pontificia Universidad Catolica del Ecuador : https://www.puce.edu.ec/intranet/documentos/Reglamentos/PUCE-SG-Dominios-Academicos-y-Lineas-de-Investigacion.pdf

Ramírez, S. X. (2020). *Aplicación de informática forense en auditorías gubernamentales para la determinación de indicios de responsabilidad penal con delitos informáticos en Ecuador.* revista de políticas y problemas públicos, vol. 2, núm. 11, 135-153.

Salazar, D., Maldonado, M. T., & Tapia, B. R. (2021). *CIBERDELITOS: perfil criminológico.* Quito: Fiscalía General del Estado.

Segundo Congreso Suramericano de Derecho Internacional Privado . (1940). *Tratado de Derecho Penal Internacional.* Montevideo: Segundo Congreso Suramericano de Derecho Internacional Privado .

Terol, M., & Chavarri, G. (8 de octubre de 2023). *La era digital, educación y trabajo: detalles de una transformación*. Obtenido de Blogthinkbig.com: https://blogthinkbig.com/la-era-digital-educacion-y-trabajo-detalles-de-una-transformacion/

Trevino, A. (22 de diciembre de 2023). *¿Qué es un «skimmer» de tarjetas de crédito y cómo puedo detectar uno?* Obtenido de Keeper Security: https://www.keepersecurity.com/blog/es/2023/12/22/what-is-a-credit-card-skimmer-and-how-can-i-spot-one/

Trigo, S., Castellote, M., Podestá, A., Ruiz de Angeli, G., Lampert, S., & Constanzo, B. (2017). *Ransomware: seguridad, investigación y tareas forenses.* Obtenido de Universidad FASTA: http://redi.ufasta.edu.ar:8082/jspui/handle/123456789/1595

Valle Matute, J. C. (Diciembre de 2013). *El delito Informático del Phishing.* Obtenido de Universiadad Regional Autónoma de los Andes. UNIANDES: https://dspace.uniandes.edu.ec/handle/123456789/2819

Villón, H. S. (2019). *Pharming y Phishing: Delitos Informáticos Penalizados por la Legislación Ecuatoriana.* Revista Ibérica de Sistemas E Tecnologias de Información, 17.