Universidad Tecnológica ECOTEC

Facultad:
Derecho y Gobernabilidad

Título del Trabajo:

El delito de apropiación fraudulenta por medios electrónicos, a través del sistema bancario y los efectos jurídicos derivados de la violación de los derechos constitucionales, período 2022 - 2023

Línea de Investigación:

Gestión de las Relaciones Jurídicas

Modalidad de Titulación:

Trabajo de Integración Curricular

Carrera:

Derecho
Énfasis en Ciencias Penales y Criminológicas

Título a obtener:

Abogado

Autor (as):

Ibis Anahí España Barandica
Ericka Karina Torres Zapata

Tutor (a):

Mgtr. María Elena Carrillo Ortega

Samborondón – Ecuador

2024

Certificado de coincidencias

CERTIFICADO DEL PORCENTAJE DE COINCIDENCIAS

Habiendo sido nombrada la Mgtr. María Elena Carrillo Ortega, tutora del Trabajo de Integración Curricular “El delito de apropiación fraudulenta por medios electrónicos, a través del sistema bancario y los efectos jurídicos derivados de la violación de los derechos constitucionales, período 2022 - 2023”, elaborado por **Ibis Anahí España Barandica y Ericka Karina Torres Zapata,** con mi respectiva supervisión como requerimiento parcial para la obtención del título de abogado.

Se informa que el mismo ha resultado tener un porcentaje de coincidencias del 7%, el mismo que se puede verificar en el print de pantalla a continuación:

MARIA ELENA CARRILLO ORTEGA

Firmado digitalmente por MARIA ELENA CARRILLO ORTEGA
Fecha: 2024.04.13 08:33:43 -05'00'

FIRMA DEL TUTOR

Mgtr. María Elena Carrillo Ortega

Certificado de aprobación tutor

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

Samborondón, 15 de abril de 2024

Magíster
Andrés Madero Poveda
Decano de la Facultad Derecho y Gobernabilidad
Universidad Tecnológica ECOTEC

De mis consideraciones:

Por medio de la presente comunico a usted que el Trabajo de Integración Curricular TITULADO: "El delito de apropiación fraudulenta por medios electrónicos, a través del sistema bancario y los efectos jurídicos derivados de la violación de los derechos constitucionales, período 2022 - 2023" fue revisado y se deja constancia que las estudiantes acogieron e incorporaron todas las observaciones realizadas por los miembros del tribunal de sustentación por lo que se autoriza a: Ibis Anahí España Barandica y Ericka Karina Torres Zapata para que procedan a la presentación del trabajo de titulación para la revisión de los miembros del tribunal y posterior sustentación.

ATENTAMENTE,

MARIA ELENA CARRILLO ORTEGA
Firmado digitalmente por MARIA ELENA CARRILLO ORTEGA
Fecha: 2024.04.13 08:36:12 -05'00'

Mgtr. María Elena Carrillo Ortega

Tutora

Dedicatoria

Con profundo reconocimiento y gratitud, dedicamos este trabajo de investigación a nuestras amadas madres, cuyo inquebrantable apoyo ha sido el sostén de nuestro camino académico y personal. Su incansable esfuerzo, dedicación y sacrificio nos han impulsado a seguir adelante en cada paso que hemos dado. Valoramos enormemente el tiempo, la energía y los recursos que han invertido para brindarnos todo lo que necesitábamos para crecer y desarrollarnos. Su amor incondicional y su infinita bondad han sido la luz que nos ha guiado en los momentos difíciles y han sido el motor que nos impulsa hacia el éxito. A nuestras madres, nuestro más sincero agradecimiento por todo lo que han hecho por nosotros y por ser el ejemplo vivo de entrega y amor incondicional. Con profundo cariño y eterna gratitud;

Ibis y Ericka.

Resumen

El avance tecnológico ha generado desafíos legales y sociales, especialmente en el ámbito bancario, donde el delito de apropiación fraudulenta por medios electrónicos, como el carding, ha proliferado. A pesar de reformas legales, persisten lagunas jurídicas en Ecuador, como la ausencia de tipificación específica para el carding. Este estudio busca identificar patrones delictivos, métodos de perpetración y vulnerabilidades en el sistema bancario, proponiendo una reforma legal para tipificar el delito de carding.

La investigación comprende un análisis comparativo con la legislación internacional, destacando la importancia de adaptar las leyes y políticas de ciberseguridad para abordar eficazmente estos delitos. Se discuten las sanciones establecidas en la legislación internacional y se propone la inclusión del delito de carding en el marco legal ecuatoriano como medida preventiva y disuasoria.

La metodología de investigación incluye entrevistas con expertos legales y en seguridad informática, así como análisis de casos judiciales y revisión bibliográfica. Los resultados muestran la necesidad de recursos y cooperación internacional para investigar y perseguir delitos electrónicos, así como la importancia de proteger los derechos constitucionales y fortalecer la seguridad cibernética en el sistema bancario.

La propuesta de reforma al artículo 190 del COIP busca cerrar la brecha legislativa y establecer pautas claras para la investigación y persecución de delitos electrónicos, mejorando la eficiencia del sistema legal y protegiendo los derechos y la privacidad de los usuarios en plataformas digitales. En conclusión, esta medida representa un importante avance en la lucha contra la ciberdelincuencia y en la defensa de la justicia y los derechos humanos en Ecuador.

Palabras claves: Delito electrónico, Carding, Reforma legal, Ciberseguridad, Protección de derechos.

Abstract

Technological advancement has brought about legal and social challenges, especially in the banking sector, where the crime of fraudulent appropriation through electronic means, such as carding, has proliferated. Despite legal reforms, legal gaps persist in Ecuador, such as the absence of specific classification for carding. This study aims to identify criminal patterns, perpetration methods, and vulnerabilities in the banking system, proposing a legal reform to classify carding as a crime.

The research involves a comparative analysis with international legislation, highlighting the importance of adapting laws and cybersecurity policies to effectively address these crimes. Sanctions established in international legislation are discussed, and the inclusion of carding as a crime in the Ecuadorian legal framework is proposed as a preventive and deterrent measure.

The research methodology includes interviews with legal and cybersecurity experts, as well as analysis of judicial cases and bibliographic review. The results demonstrate the need for resources and international cooperation to investigate and prosecute electronic crimes, as well as the importance of protecting constitutional rights and strengthening cybersecurity in the banking system.

The proposed reform to Article 190 of the COIP aims to close the legal gap and establish clear guidelines for the investigation and prosecution of electronic crimes, improving the efficiency of the legal system and protecting the rights and privacy of users on digital platforms. In conclusion, this measure represents a significant advancement in the fight against cybercrime and the defense of justice and human rights in Ecuador.

Keywords: Electronic crime, Carding, Legal reform, Cybersecurity, Rights protection.

Índice

Introducción

En la era digital, el avance vertiginoso de la tecnología a nivel mundial, ha traído consigo no sólo beneficios evidentes, sino también desafíos legales y sociales que requieren de una atención meticulosa para su investigación. Dentro de este panorama, el delito de apropiación fraudulenta por medios electrónicos, particularmente a través del sistema bancario, se ha convertido en un fenómeno de creciente preocupación.

En el contexto jurídico ecuatoriano, el análisis respecto al cometimiento del delito de apropiación fraudulenta por medios electrónicos, emerge por la rápida expansión de las transacciones electrónicas y la creciente interconexión tecnológica que han dado lugar a un incremento significativo de prácticas delictivas, destacándose la apropiación fraudulenta como una amenaza latente dentro de los espacios cibernéticos.

En el Ecuador, durante los años 2022 y 2023 se dió la proliferación en el cometimiento de un delito electrónico denominado carding, mismo que consiste en la utilización no autorizada por parte de los propietarios de sus tarjetas de débito o crédito bancario, a fin de realizar transacciones, sin el consentimiento previo de estos, mediante la utilización de sistemas informáticos o mejor conocidos como Malware.

Los delincuentes que realizan esta práctica mediante el uso no autorizado de tarjetas bancarias, son conocidos como "carders", mismos que a su vez se encargan de recopilar información de ellas de forma ilegal; mediante la piratería o mejor denominado como skimmer, técnica que consiste es la utilización de un dispositivo en los cajeros automáticos a través de la clonación de la banda magnética que poseen las tarjetas bancarias.

O mediante el phishing, técnica que implica el envío masivo de correos electrónicos fraudulentos que tienen la apariencia de genuinos, los cuales son enviados por los delincuentes informáticos o denominados estafadores.

Por ello, a lo largo de esta investigación, se abordarán aspectos claves, como lo son el desarrollo tecnológico utilizado por los ciberdelincuentes, las respuestas legales y judiciales a estos delitos, así como los impactos que tienen en la vulneración de derechos humanos.

En el presente trabajo de investigación, analizará de cerca el régimen legal en Ecuador con respecto a este tipo de delito, ya que es necesario considerar la complejidad de las estrategias aplicadas por los ciberterroristas y también la urgencia de reformar las leyes para los desafíos que se enfrentan en el mundo actual referente al cometimiento de este tipo de delitos.

El propósito de este trabajo es contribuir a una mayor comprensión de esta problemática ilícita. Por ello, proporcionará una base sólida sobre la cual se pueden sentar pilares para la construcción de mejores marcos legales y adoptar estrategias determinantes, a fin de garantizar la protección de los derechos constitucionales en entornos digitales y bancarios.

Contexto histórico

Con el boom de la era de la banca electrónica, se comenzó a facilitar a los clientes la realización de transacciones financieras sin demora; esto trajo consigo una mayor facilidad y accesibilidad para los usuarios al momento de ejecutarlas.

Desde la década de los años de 1970 al 1980, cuando se dio la introducción de la Banca Electrónica, mediante la implementación de herramientas tecnológicas como cajeros automáticos y transferencias electrónicas, mismas que a su vez crearon nuevas posibilidades y problemas para la industria bancaria. A partir de ello, comenzaron a desarrollarse formas primitivas de fraude electrónico, pero no tan desarrolladas como las conocemos hoy en día.

Es en el año de 1990 con la expansión del Internet, fue acompañada a su vez por transacciones en línea más numerosas que dieron lugar a innumerables casos de fraude electrónico. Los delincuentes no dudaron en utilizar trucos como el phishing para obtener información privada de los usuarios.

Desde el año 2000, cuando hubo avances significativos en tecnología como servicios en línea y aplicaciones móviles, han surgido una nueva gama de amenazas que incluyen malware, que se refieren a programas informáticos destinados a causar daños o realizar operaciones indeseables en un sistema informático; ransomware, desarrollado como una forma de cifrar archivos en el sistema de una víctima y posteriormente exigir el pago de un rescate; y otras formas de fraude que se transformaron después de que se explotaron los puntos débiles de estos sistemas.

Desde el año 2010 hasta el presente, la tasa de crecimiento de los delitos cibernéticos, evolucionó hasta convertirse en una amenaza global más avanzada. Comenzaron a producirse con regularidad incidentes de importantes penetraciones en el sistema bancario que implican intrusiones considerables, filtración de datos, así como robo de dinero y fraude.

Con la llegada de la inteligencia artificial y la automatización, también contribuyeron a ataques avanzados a las tecnologías de la información que se volvieron más efectivos debido a la rápida evolución de la tecnológica. Por ello, es crucial que los sistemas bancarios adopten

medidas de seguridad tomando en cuenta el marco legal vigente, a fin de combatir la creciente ola de delitos cibernéticos.

Antecedentes

El uso fraudulento de las tarjetas de crédito o débito tiene sus raíces en la década de 1950, cuando se crearon las primeras tarjetas. Sin embargo, el término "carding" y las prácticas modernas asociadas con él se desarrollaron con la expansión del internet y del comercio electrónico.

Dentro del Ecuador se realizaron varias reformas al Código Orgánico Integral Penal (COIP) y se incorporó disposiciones específicas sobre delitos informáticos o delitos electrónicos; esto incluye disposiciones relacionadas con el acceso no autorizado a sistemas informáticos, la interceptación de comunicaciones electrónicas, el sabotaje informático, la apropiación fraudulenta por medios electrónicos, entre otros.

La inserción de estos delitos electrónicos en el COIP demuestra la creciente importancia de abordar las actividades delictivas en el ámbito digital y proteger la seguridad y la integridad de los usuarios. La normativa busca adaptarse a los avances tecnológicos, proporcionando un marco legal adecuado para sancionar las conductas delictivas relacionadas con la tecnología.

Conforme al principio de legalidad estipulado en el art. 5 numeral 1 del COIP, las normas penales deben estar establecidas dentro de la ley para que se pueda juzgar el delito; sin embargo, según boletín emitido en agosto del 2022 por la Policía Nacional del Ecuador se habla sobre el delito del carding, el cual no se encuentra tipificado en el ordenamiento jurídico penal ecuatoriano.

Aunque en el Ecuador se han realizado varias reformas legales para incluir disposiciones sobre delitos electrónicos, aún persisten lagunas legales, como la ausencia de una tipificación específica para el carding. Esta brecha resalta la importancia de una revisión continua de las leyes para mantenerse al día con los avances tecnológicos y garantizar la protección y seguridad jurídica de las personas.

Planteamiento del Problema

El análisis y procesamiento de resultados de la investigación sobre el delito de apropiación fraudulenta por medios electrónicos en el sistema bancario y sus implicaciones jurídicas en la violación de derechos constitucionales se llevará a cabo mediante entrevistas

a profesionales del derecho especializados en el tema. Las opiniones recogidas se tabularon y posteriormente se presentaron de manera resumida mediante la realización de tablas que permitieran obtener un análisis más detallado.

Del mismo modo, este fenómeno delictivo no sólo pone de manifiesto la sofisticación de las técnicas empleadas por los infractores al momento de cometerlos. Por otro lado, se evidenciará las vulnerabilidades inherentes presentes en la realización de transacciones electrónicas en los sistemas bancarios nacionales. Con ello, se plantean interrogantes cruciales sobre la capacidad del marco jurídico existente para hacer frente a esta nueva modalidad delictiva.

Se espera identificar los posibles patrones y tendencias de conductas relativas del cometimiento de estos tipos de delitos o los comportamientos inherentes de los denominados "carders " al obtener información de tarjetas de débito o crédito para robar los fondos de sus dueños, así como las consecuencias que esto genera en la persona afectada. Además, se discutirá cómo estos actos ponen en vulneración el sistema jurídico, que hasta cierto punto no respalda el sometimiento de tales acciones.

Objetivos

Objetivo General:

Determinar las dimensiones jurídicas del delito de apropiación fraudulenta por medios electrónicos, a través de un análisis de los casos presentados, así como los efectos derivados de la violación de los derechos constitucionales de las personas afectadas, para comprender el alcance y la complejidad jurídica del delito.

Objetivos Específicos:

1. Identificar los métodos o patrones de ejecución del delito de apropiación fraudulenta por medios electrónicos, mediante la recopilación de datos y la investigación de casos previos, con el propósito de comprender cómo se lleva a cabo y para qué se utiliza esa información.
2. Desarrollar un estudio jurídico comparado con la legislación internacional, a través del análisis de la normativa relacionada con este delito en otros países, para determinar los beneficios de su aplicabilidad en la legislación penal ecuatoriana.

3. Proponer una reforma al Código Orgánico Integral Penal, mediante la tipificación del delito de Carding, con el fin de garantizar la seguridad jurídica de los usuarios que se ven afectados por estos ciberdelitos.

Justificación

La justificación de este tema de investigación, respecto al delito de apropiación fraudulenta por medios electrónicos a través del sistema bancario y los efectos jurídicos que resultan de la violación de derechos constitucionales en relación al cometimiento de estos delitos, están motivados por la alta demanda contemporánea con el fin de comprender y afrontar los desafíos que surgen en el ámbito jurídico y tecnológico actual.

En primer lugar, la alta incidencia en la realización de transacciones electrónicas y la dependencia del sistema bancario respecto a las operaciones financieras, dan a lugar la necesidad de comprender de manera profunda, las amenazas que representan los delitos cibernéticos relativos al tema de la seguridad y la confianza en los bancos. Por ello, la identificación de patrones delictivos, métodos de perpetración y vulnerabilidades dentro de estos sistemas, se convierten en una tarea crucial para desarrollar estrategias efectivas de prevención y enjuiciamiento al cometimiento de estas conductas.

Además, la salvaguardia de derechos constitucionales dentro de esta esfera digital es imprescindible, ya que es parte integral de una sociedad interconectada que está en continuo crecimiento. Despojar a las personas de su privacidad, seguridad financiera y otros derechos básicos mediante el robo electrónico cuestiona el valor de los sistemas legales establecidos y su adaptación a la situación tecnológica actual.

La investigación propuesta busca contribuir en el campo de la creación de nuevos conocimientos a fin de brindar estudios exhaustivos respecto a cuestiones legales y tecnológicas de este tipo de delito. Además de eso, también establecerá soluciones prácticas a fin de reforzar las leyes y salvaguardar los derechos en relación con el robo a través de dispositivos electrónicos con miras a promover la confianza en los sistemas financieros digitales.

Marco Teórico

Análisis del Delito de Apropiación Fraudulenta por Medios Electrónicos en el Ecuador.

Definición y características del delito de apropiación fraudulenta por medios electrónicos.

En la actualidad, la sociedad está inmersa en la era de la tecnología, donde las personas están constantemente expuestas a los diversos peligros que acechan en internet, un vasto mundo lleno de posibilidades y riesgos. Los delitos informáticos han evolucionado considerablemente, dando lugar a “prácticas como el hacking, el sabotaje de datos y programas, la interceptación no autorizada de información a través de dispositivos tecnológicos, el espionaje en línea, entre otros” (Gómez, 2022, pág. 11).

El sabotaje informático se ha convertido en una preocupación creciente, ya que se pueden alterar datos cruciales o desactivar sistemas esenciales para el funcionamiento de empresas e instituciones.

> La interceptación no autorizada de información ya sea mediante el uso de "malware" o técnicas de ingeniería social, es otro peligro que puede resultar en la exposición de datos sensibles como contraseñas, números de tarjetas de crédito y detalles bancarios (Sain, 2015, pág. 1).

Según Yari (2023), “los actos delictivos en general comprenden acciones contrarias a la ley, típicamente descritas en normativas legales que suelen abordar conductas como robo, estafa, defraudación, entre otros” (p. 8).

Antes de la revolución tecnológica que el mundo ha experimentado, estos tipos de delitos eran analizados por la teoría penal desde una sola perspectiva. Sin embargo, las demandas de la sociedad actual han forzado a que la legislación penal evolucione hacia el ámbito virtual, dando así origen a los delitos electrónicos.

Por otro lado, una definición realizada por Acurio (2012), en la que estipula lo siguiente: “los delitos informáticos se refieren a aquellos crímenes en los que se utiliza un sistema automatizado para procesar o transmitir datos” (p. 2). Aunque esta definición es bastante amplia y general, estos delitos suelen ser vistos desde la perspectiva de cómo se emplea la tecnología para llevar a cabo actividades delictivas.

Algunos expertos los describen como acciones típicas, contrarias a la ley, con culpabilidad y castigo en el ámbito de los sistemas informáticos; ya sea que estos sistemas

sean utilizados como herramienta para cometer un delito o que el delito mismo se dirija hacia el sistema informático en sí.

De conformidad a lo manifestado por los autores Marcelo Huerta y Claudio Líbano definen los delitos informáticos como:

> Todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual, generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro." (Huerta & Líbano, 1996, pág. 17)

Como se evidenció en los párrafos previos, la apropiación fraudulenta por medios electrónicos es un delito perpetrado mediante dispositivos electrónicos o informáticos con el propósito de obtener de manera engañosa dinero, bienes o datos pertenecientes a otra persona sin su autorización.

Fundamentalmente, implica la utilización indebida de información electrónica para obtener beneficios ilegítimos a expensas de la víctima. En términos prácticos, puede manifestarse de diversas maneras, como la transferencia fraudulenta de fondos, el robo de identidad en línea, el acceso no autorizado a cuentas bancarias o sistemas informáticos, entre otras modalidades. El elemento central es la realización de una apropiación indebida mediante el uso de la tecnología como medio para cometer el fraude.

Una vez que se han establecido los principios teóricos de los delitos informáticos, resulta pertinente analizar las particularidades o características distintivas que los definen para una comprensión más profunda. Es crucial destacar que, a diferencia de otros actos ilícitos que pueden ser perpetrados por cualquier persona, los delitos informáticos requieren la intervención de individuos con un alto nivel de conocimiento en tecnología, ya que se consideran delitos de "*cuello blanco".*

Entre las particularidades que exhiben los delitos informáticos, se resalta la rapidez con la que se llevan a cabo, la distancia que puede existir entre el lugar del acto ilegal y donde se manifiesta el resultado, así como la dificultad para identificar a los responsables, quienes poseen la habilidad de eliminar evidencias o modificar programas y datos sin dejar rastros, asegurando su escape de la justicia.

Asimismo, una de las características sobresalientes en estos delitos es la flexibilidad en tiempo y espacio, ya que no requieren de un lugar físico para concretarse, lo cual complica

la verificación de dicha actividad ilícita. En último término, “suelen provocar pérdidas económicas considerables, especialmente a entidades financieras y sus usuarios que emplean sus plataformas digitales” (Torres, 2022, pág. 9).

> Esto subraya un aspecto significativo, dado que los perpetradores de estos actos delictivos poseen un amplio conocimiento en el ámbito de la informática, e incluso en algunos casos, están situados en posiciones que les permiten acceder a datos sensibles, ocasionando perjuicios económicos en la mayoría de las ocasiones (Torres, 2022, pág. 9).

Ante esta situación, es frecuente que tales conductas no sean investigadas, o incluso peor, que no sean denunciadas ante las autoridades pertinentes, debido al alto grado de impunidad que prevalece en estos casos por la falta de una legislación que penalice estas actividades.

Técnicas utilizadas en el cometimiento del delito de apropiación fraudulenta por medios electrónicos.

La apropiación fraudulenta por medios electrónicos es un delito que involucra el uso indebido de información o acceso a sistemas electrónicos para obtener beneficios financieros de manera ilegítima. Algunas de las técnicas comúnmente utilizadas en la comisión de este delito incluyen:

Phishing.

El phishing es una técnica de ingeniería social donde los delincuentes envían correos electrónicos o mensajes de texto que aparentan ser de instituciones legítimas, como bancos, compañías de tarjetas de crédito o servicios en línea populares. Estos mensajes suelen incluir enlaces a sitios web falsos que se asemejan a los legítimos.

> El objetivo es engañar a las víctimas para que revelen información personal o financiera, como contraseñas, números de tarjetas de crédito, números de seguridad social, etc. Una vez que la víctima proporciona esta información, los delincuentes la utilizan para acceder a sus cuentas y realizar transacciones fraudulentas. (Hernández, 2023, pág. 196).

Malware.

El malware, abreviatura de "software malicioso", es un tipo de software diseñado para dañar, acceder o tomar el control de un sistema informático sin el consentimiento del usuario. Los delincuentes pueden distribuir malware a través de “correos electrónicos con archivos adjuntos infectados, descargas en línea, anuncios maliciosos o incluso dispositivos” USB infectados (Belcic, 2023, pág. 1).

Una vez que el malware infecta el dispositivo de la víctima, puede registrar las pulsaciones del teclado para robar contraseñas, acceder a información confidencial almacenada en el dispositivo o incluso tomar el control completo del sistema. Esta información luego se utiliza para realizar transacciones fraudulentas o acceder a cuentas bancarias.

Pharming.

El pharming es una técnica más sofisticada donde los delincuentes redirigen el tráfico de internet de las víctimas hacia sitios web falsos, incluso cuando las víctimas ingresan la dirección correcta en su navegador. "Esto se logra mediante la manipulación de los servidores DNS (Sistema de Nombres de Dominio) o mediante la instalación de malware en el dispositivo de la víctima" (Patiño Corona, 2009, pág. 23).

Estos sitios web falsos suelen ser réplicas exactas de sitios legítimos, como bancos o servicios de pago en línea. Una vez que las víctimas ingresan su información de inicio de sesión en estos sitios falsos, los delincuentes pueden capturar esta información y utilizarla para acceder a las cuentas reales de las víctimas y realizar transacciones no autorizadas.

Ingeniería social.

La ingeniería social es una técnica que implica manipular a las personas para que revelen información confidencial o realicen ciertas acciones. Los delincuentes pueden hacerse pasar por empleados de una empresa, representantes de servicios técnicos, amigos en redes sociales u otras identidades de confianza para engañar a las víctimas.

> Pueden utilizar el correo electrónico, llamadas telefónicas, mensajes de texto o redes sociales para obtener información sensible, como contraseñas, códigos de verificación, respuestas a preguntas de seguridad, entre otros. Una vez que obtienen esta información, pueden usarla para acceder a cuentas en línea, realizar cambios en la configuración de seguridad o llevar a cabo actividades fraudulentas en nombre de la víctima (García, 2020, pág. 11).

Es crucial que las personas mantengan una conciencia activa sobre estas técnicas y adopten medidas para salvaguardar su información personal y financiera. Esto implica ejercer precaución al proporcionar datos en línea, emplear software antivirus y mantenerse actualizados sobre las amenazas cibernéticas emergentes. Además, las instituciones financieras y empresas deben implementar medidas de seguridad sólidas para resguardar a sus clientes y usuarios contra los delitos electrónicos de esta índole.

Respuestas legales frente a los casos de apropiación fraudulenta por medios electrónicos.

La estructura del sistema judicial en Ecuador se expone detalladamente en el Código Orgánico Integral Penal. Este sistema se divide principalmente en dos fases: una previa al juicio y otra orientada a establecer los elementos esenciales para imponer una sanción a un individuo específico debido a una acción delictiva.

La fase previa al proceso penal se compone principalmente de la fase de investigación judicial, que comienza tan pronto como el fiscal, encargado del control de la acción penal, toma conocimiento del delito.

Este conocimiento puede adquirirse a través de denuncias presentadas ante la Fiscalía General del Estado, la Policía Nacional, o el personal del Sistema Integral, o bien, mediante informes de supervisión elaborados por entidades de control como la Contraloría General. Además, las decisiones judiciales, como resoluciones y fallos emitidos por jueces o tribunales con relevancia penal, también pueden desencadenar este proceso.

Una vez que el fiscal obtiene conocimiento, se inicia la investigación preliminar, cuyo objetivo principal es determinar si el acto en cuestión constituye un delito según lo establecido por la ley. Durante esta fase, se buscan pistas sobre cómo ocurrió el acto, sus motivaciones y se intenta establecer conexiones entre estas pistas y posibles sospechosos vinculados a la acción investigada.

El fiscal tiene un plazo de uno o dos años, dependiendo de la gravedad del delito en cuestión. En el caso de desapariciones, “el proceso no puede cerrarse hasta que la persona aparezca, o las pistas reunidas sean suficientes para señalar a un sospechoso por el delito en consideración” (Yari, 2023, pág. 26).

Una vez concluida la etapa de investigación y confirmada la existencia de un delito penal, se inicia la fase de instrucción fiscal, conocida por convocar a los sospechosos para el proceso de formulación de cargos. En este período, tanto la fiscalía como los sospechosos tienen la oportunidad de presentar sus argumentos y pruebas con el objetivo de persuadir al juez sobre si deben o no enfrentar cargos penales.

En el contexto de este análisis, centrado principalmente en los mecanismos que la ley utiliza para identificar al perpetrador, estas dos fases se consideran fundamentales. En Ecuador, el proceso penal culmina con la audiencia preparatoria de juicio y el juicio mismo,

donde se emite una sentencia en caso de que se establezca la responsabilidad o no del acusado.

Marco jurídico y normativo relativo al Delito de Apropiación Fraudulenta por Medios Electrónicos.

Principios constitucionales vulnerados por el cometimiento del delito de Apropiación Fraudulenta por medios electrónicos.

El delito de Apropiación Fraudulenta por medios electrónicos en Ecuador vulnera varios principios constitucionales fundamentales. En primer lugar, atenta contra el principio de legalidad, el cual establece que nadie puede ser sancionado por acciones u omisiones que no estén tipificadas como delito en la ley. Al cometerse este delito, “se está violando este principio al utilizar medios electrónicos para apropiarse de manera ilícita de bienes o recursos, lo que no está permitido por la ley (Constitución de la República del Ecuador, 2008, pág. 74).

Además, este tipo de delito vulnera el principio de seguridad jurídica, que garantiza que las personas puedan confiar en que sus derechos y bienes estarán protegidos por la ley. La Apropiación Fraudulenta por medios electrónicos genera inseguridad en el ámbito digital, donde las personas pueden ser víctimas de acciones fraudulentas sin tener la certeza de que habrá una protección legal efectiva.

Otro principio afectado es el de igualdad ante la ley, dado que “este delito puede afectar a personas de diversos sectores de la sociedad, sin importar su condición social, económica o laboral” (Constitución de la República del Ecuador, 2008, pág. 90). Todos están expuestos a ser víctimas de este tipo de apropiación fraudulenta, lo que socava el principio de igualdad al generar desigualdades en términos de seguridad y protección de bienes.

Es decir que, la Apropiación Fraudulenta por medios electrónicos en Ecuador vulnera los principios constitucionales de legalidad, seguridad jurídica e igualdad ante la ley, al utilizar medios digitales para cometer actos ilícitos que afectan a la población en general.

Disposiciones legales relativas a los derechos de los usuarios afectados por la vulneración de sistemas electrónicos.

De conformidad a lo estipulado en la Ley Orgánica de Protección de Datos Personales (LOPDP) en su artículo 1, manifiesta que:

> Objeto y finalidad. - El objeto y finalidad de la presente ley es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección, Para dicho efecto regula, prevé y desarrolla principios, derechos, obligaciones y mecanismos de tutela. (Ley Orgánica de Protección de Datos Personales, 2021, p. 5)

Por otro lado, la LOPDP en su primer artículo tiene como objetivo:

> El presente Código tiene por objeto establecer los principios y reglas que rigen el ejercicio y protección de los derechos del usuario del sistema financiero, considerando que las actividades financieras son de orden público y deben sujetarse, en particular, a principios de sanas prácticas aplicadas por el gobierno corporativo de las instituciones que conforman el sistema financiero. Su ámbito de aplicación involucra las relaciones entre los usuarios y las instituciones financieras controladas por la Superintendencia de Bancos y Seguros del Ecuador, sin perjuicio de otras disposiciones legales que contemplen medidas e instrumentos de protección al usuario del sistema financiero. Para los propósitos de este Código, los términos jurídicos, contenidos en su texto, deberán entenderse de conformidad al glosario que consta en el artículo final. (Resolución No. JB-2010-1782, 2010, pág. 1)

Medidas de protección para garantizar los derechos de las víctimas afectadas por delitos electrónicos.

En Ecuador, las leyes contemplan varias medidas de protección para garantizar los derechos de las víctimas afectadas por delitos electrónicos. Estas medidas se enfocan en brindar apoyo y seguridad a las personas que han sido víctimas de este tipo de delitos, reconociendo la importancia de proteger su integridad y sus derechos.

Una de las medidas clave es el acceso a la justicia y a la asistencia legal. Las víctimas de delitos electrónicos tienen derecho a recibir asesoramiento jurídico y apoyo para comprender el proceso legal en el que están involucradas. “Esto puede incluir información sobre cómo presentar denuncias, participar en investigaciones y acceder a recursos legales” (Campos, 2014, pág. 1).

> Además, se busca preservar la privacidad y seguridad de las víctimas. Las leyes ecuatorianas contemplan medidas para proteger la información personal de las personas afectadas por delitos electrónicos, evitando que su identidad o datos sensibles sean divulgados de manera inapropiada durante investigaciones o procesos legales (Campos, 2014, pág. 1).

Otra medida importante es el apoyo psicológico y emocional. Las víctimas de delitos electrónicos pueden experimentar traumas y efectos emocionales negativos, por lo que se promueve el acceso a servicios de apoyo psicológico para ayudarles a sobrellevar las consecuencias de estos actos.

Asimismo, se contempla la reparación del daño. Por otra parte, las leyes ecuatorianas buscan que “las víctimas de delitos electrónicos reciban compensación por los daños y perjuicios sufridos. Esto puede incluir la restitución de bienes o la reparación económica por los daños materiales o morales ocasionados” (Argudo, 2018, pág. 8).

En resumen, las medidas de protección para las víctimas de delitos electrónicos en Ecuador incluyen el acceso a la justicia y asistencia legal, la protección de la privacidad, el apoyo psicológico y la reparación del daño. Estas medidas buscan asegurar que las personas afectadas reciban el apoyo necesario para superar las consecuencias de estos delitos y puedan ejercer sus derechos de manera adecuada.

Estudio de Derecho comparado de la Legislación Penal Ecuatoriana con la Legislación Internacional en los Casos de Carding

Con la legislación argentina

El "carding" es una práctica delictiva que involucra el robo de información financiera y su uso fraudulento en transacciones en línea. Es importante analizar cómo la legislación penal ecuatoriana y argentina abordan este tema.

En Ecuador, el COIP, contempla disposiciones relacionadas con delitos informáticos, incluyendo aquellos vinculados al carding. Por ejemplo, el Art. 234 tipifica “el acceso no autorizado a sistemas informáticos, lo cual podría aplicarse en casos de carding cuando se accede a información bancaria de manera ilegal” (Código Orgánico Integral Penal, 2014, pág. 90). Además, el artículo 236 sanciona “la interceptación de datos informáticos, que también puede estar relacionado con el carding si se obtiene información de tarjetas de crédito de forma ilícita” (Código Orgánico Integral Penal, 2014, pág. 91).

Por su parte, Código Penal de la Nación Argentina (CPNA), incluye disposiciones que abordan aspectos similares. El artículo 153 establece “penas para quien acceda indebidamente a un sistema o dato informático, mientras que el artículo 157 tipifica la interceptación de comunicaciones electrónicas” (Código Penal de la Nación Argentina, 1984, pág. 16). Estos artículos podrían aplicarse en casos de carding donde se obtiene y utiliza información financiera de manera fraudulenta.

En un análisis jurídico comparado entre la legislación penal ecuatoriana y argentina en casos de carding, se observan similitudes y diferencias destacadas, tomando en consideración casos emblemáticos. En Argentina, el caso de Fernando Falsetti, conocido

como el "canillita hacker", revela la paradoja de un individuo que, de manera analógica, ejecutó más de un centenar de estafas con tarjetas de crédito, utilizando un algoritmo manual para generar números de tarjetas y códigos de seguridad.

Este caso subraya “la necesidad de abordar las amenazas cibernéticas desde una perspectiva integral que incluya tanto métodos tradicionales como digitales” (El Tiempo, 2022, p. 1).

Por otro lado, en Ecuador, un estudio realizado a 30 profesionales del ámbito jurídico expone deficiencias en la legislación y la respuesta institucional ante delitos informáticos. La falta de socialización sobre las leyes y derechos informáticos contribuye a que “las denuncias no se tomen en serio, y la ausencia de una adecuación de conductas nocivas en el código penal resulta en una alta proporción de casos catalogados como cifras negras” (Tráves, 2018 , p. 48). Además, se señala que la falta de profesionales capacitados para actuar ante delitos informáticos representa “un desafío significativo, evidenciado por casos como el de Villavicencio y WikiLeaks, así como el terrorismo informático de Anonymous en 2010” (Arias & Manzano, 2023, p. 142).

Ambas jurisdicciones enfrentan desafíos comunes, como la falta de profesionales especializados y la necesidad de fortalecer la telemática y la respuesta institucional para abordar eficazmente la ciberdelincuencia. En este contexto, las mejoras en la legislación, la sensibilización sobre derechos informáticos y la capacitación de profesionales en ciberseguridad son elementos cruciales para combatir los casos de carding y otros delitos cibernéticos en ambas naciones.

La cooperación internacional también se presenta como esencial, considerando la naturaleza transfronteriza de los delitos cibernéticos. En última instancia, la adaptabilidad de la legislación a las evoluciones tecnológicas y la asignación de recursos para fortalecer la capacidad de respuesta son aspectos fundamentales para garantizar la eficacia en la lucha contra la ciberdelincuencia en Argentina y Ecuador.

Con la legislación mexicana

En México, el delito de carding está contemplado en el Código Penal Federal (en adelante CPE) en el artículo 211 Bis, el cual establece “penas para quien ilegalmente y sin consentimiento de su titular, obtenga, compile, conserve, divulgue, comercialice, transmita, distribuya o utilice de cualquier forma datos personales, financieros o patrimoniales de una persona física o moral” (Código Penal Federal , 2018, pág. 50).

Este artículo fue adicionado al CPE en 2014 para abordar específicamente los delitos informáticos y la creciente problemática del carding en el país. El objetivo es proteger la privacidad y seguridad de la información de los ciudadanos y las instituciones financieras.

Las penas por el delito de carding en México pueden ser de 3 a 6 años de prisión y multas de hasta 600 días de salario mínimo, dependiendo de la gravedad del caso y los daños causados. Además, si el delito se comete utilizando información obtenida de manera ilegal de bases de datos personales, las penas pueden aumentar hasta en una mitad.

Ahora bien, en un estudio comparado entre la legislación penal ecuatoriana y mexicana en relación con los casos de carding, se revelan notables divergencias y similitudes en la forma en que ambas naciones abordan los delitos cibernéticos.

En México, el modus operandi del carding implica la utilización de diversas estrategias, desde el envío de correos electrónicos fraudulentos que imitan a entidades bancarias hasta el empleo de programas y algoritmos para obtener información confidencial de tarjetas de crédito. Se destaca, además, la práctica de llamadas telefónicas fraudulentas que simulan ser instituciones bancarias para obtener datos sensibles de las víctimas.

A pesar de la “existencia de mecanismos de contracargo para proteger a los tarjeta-habientes, se evidencia una falta de tipificación penal específica para el carding, dejando impune la conducta del ciberdelincuente” (Aboitiz, 2023, p. 5).

En contraste, en Ecuador, la problemática de la ciberdelincuencia se manifiesta a través de una variedad de amenazas, desde malware para la minería de criptomonedas hasta ataques de ransomware y phishing. Se destacan casos recientes, como el ciberataque al Banco Pichincha y al Municipio de Quito, que revelan la vulnerabilidad de las instituciones frente a estos eventos. A pesar de un aumento significativo en el número de incidentes reportados, “la legislación penal ecuatoriana aún no aborda de manera específica el carding como una modalidad delictiva” (Arias & Manzano, 2023, p. 142).

En conclusión, tanto en México como en Ecuador, la ciberdelincuencia presenta desafíos significativos, desde la falta de tipificación específica para el carding hasta la necesidad de fortalecer la protección legal contra distintas amenazas cibernéticas. Ambas naciones deben considerar el rápido avance tecnológico y la creciente sofisticación de los ataques para adecuar y fortalecer sus marcos legales, promoviendo así una respuesta más efectiva ante los delitos informáticos y protegiendo los bienes jurídicos de sus ciudadanos. La cooperación internacional y la implementación de medidas preventivas son esenciales en este contexto dinámico y desafiante.

Con la legislación colombiana

En Colombia, el delito de carding se encuentra contemplado en la Ley 1273 de 2009, la cual tipifica los delitos informáticos en el país. Específicamente, el artículo 269A del Código Penal Colombiano, establece que “quien sin autorización y de manera fraudulenta obtenga, capture, intercepte, intervenga, modifique, destruya o divulgue información financiera, datos contenidos en medios informáticos o datos de comunicaciones electrónicas, incurrirá en este delito” (Código Penal Colombiano, 2009, pág. 67).

Este artículo busca proteger la integridad y seguridad de la información financiera y personal de los ciudadanos colombianos frente a prácticas fraudulentas como el carding. Se considera una conducta punible el acceso indebido a sistemas informáticos y la manipulación o divulgación no autorizada de datos financieros.

Las penas por el delito de carding en Colombia pueden ser de prisión de 48 a 108 meses y multas de 100 a 1.000 salarios mínimos legales mensuales vigentes, dependiendo de la gravedad del caso y los perjuicios ocasionados. Además, “si se comete el delito utilizando información obtenida de manera ilegal de bases de datos personales, las penas pueden aumentar hasta en una mitad” (Caldas, 2020, pág. 1).

Por otra parte, al realizar un análisis comparado entre la legislación penal ecuatoriana y colombiana en casos de carding, se identifican diferencias significativas en la forma en que ambas naciones abordan los delitos cibernéticos.

En Colombia, se observa una diversidad de delitos relacionados con la ciberseguridad, como el hurto por medios electrónicos, la irrupción informática, la suplantación de identidad y la estafa por redes sociales.

Estos delitos están tipificados en el Código Penal Colombiano, abarcando desde transferencias no consentidas de fondos hasta acceso abusivo a sistemas informáticos. Las penas varían en función de la gravedad del delito, con sanciones que “incluyen multas económicas y períodos de prisión que van desde meses hasta años, dependiendo de la naturaleza del delito” (Acosta, 2021, p. 1).

En Ecuador, la ciberseguridad se aborda desde una perspectiva más amplia, considerando la protección del ciberespacio como el quinto dominio. A través de políticas como la Política Nacional de Ciberseguridad (PNC) y la Estrategia Nacional de Ciberseguridad, el país busca fortalecer sus capacidades y responder a amenazas como el ciberterrorismo y ciberdelincuencia.

Sin embargo, aún persisten desafíos, como “la falta de medidas cooperativas y organizativas, según la evaluación de la Global Cybersecurity Index. Se destaca la atención especial a la protección de infraestructura crítica digital y servicios esenciales” (Arias & Manzano, 2023, p. 143).

En conclusión, mientras Colombia aborda de manera detallada diversas modalidades de ciberdelitos en su legislación, Ecuador se enfoca en fortalecer sus capacidades de ciberdefensa y ciberseguridad a través de políticas específicas. Ambos países enfrentan desafíos, desde la tipificación precisa de delitos hasta la necesidad de fortalecer la cooperación y las medidas organizativas.

La protección del ciberespacio y la respuesta efectiva a los ataques cibernéticos requieren una continua evolución de las políticas y marcos legales, así como la colaboración entre actores estatales y privados, tanto a nivel nacional como internacional.

Sanciones establecidas en la legislación internacional para el delito de Carding

La proliferación de actividades delictivas en el ámbito cibernético ha llevado a una creciente atención internacional sobre la necesidad de establecer sanciones efectivas para combatir delitos como el carding. El carding, definido como el uso ilegal de información de tarjetas de crédito para realizar transacciones fraudulentas, ha generado preocupaciones globales en materia de seguridad financiera y protección de datos. En respuesta a esta amenaza, la legislación internacional ha comenzado a abordar de manera específica el delito de carding, estableciendo sanciones y medidas para disuadir y castigar a quienes participan en estas prácticas ilícitas.

A continuación, se examinará detalladamente la normativa internacional en lo que respecta al delito de carding. Este análisis se centrará en las disposiciones y sanciones establecidas a nivel global para abordar la problemática del uso ilegal de información de tarjetas de crédito, comúnmente conocido como carding.

Organismos Internacionales

La creciente preocupación por el ciberterrorismo ha llevado a una acción internacional coordinada para abordar este desafío. La Unión Internacional de Telecomunicaciones (UIT), establecida por la Organización de Naciones Unidas (ONU) en 1985, desempeña un papel crucial en el desarrollo de normativas técnicas para

facilitar la interconexión de redes y tecnologías, promoviendo el acceso a las Tecnologías de la Información y Comunicación (TIC) y la gobernanza de Internet.

A nivel europeo, la Unión Europea (UE) fundó la Agencia de la Unión Europea para la Ciberseguridad (ENISA) en 2004, con la misión de fortalecer la ciberseguridad en Europa.

En América, la Organización de Estados Americanos (OEA) ha impulsado iniciativas como el Comité Interamericano contra el Terrorismo (CICTE), que estableció un programa de ciberseguridad para colaborar con los Estados miembros en el fortalecimiento de capacidades.

Además, diversas organizaciones como la Comisión Internacional de Telecomunicaciones (CITEL), la Reunión de Ministros de Justicia de América (REJMA), la Junta Interamericana de Defensa (JID), y la Fundación Interamericana de Defensa están trabajando en la formulación de normativas y estrategias para proteger el ciberespacio en la región. Destacan Argentina y Colombia como pioneros en implementar políticas y estrategias de ciberseguridad y ciberdefensa.

Legislación Argentina

En el marco jurisdiccional argentino, se abordarán las sanciones establecidas para el delito de carding, explorando los artículos pertinentes que delinean las medidas legales y punitivas aplicables a aquellos involucrados en prácticas ilícitas vinculadas con el carding.

En el Código Penal de la Nación Argentina, en el Art. 153, manifiesta lo siguiente:

> Se establecen sanciones penales para quienes accedan indebidamente a comunicaciones electrónicas o documentos privados, abriendo, apropiándose, suprimiendo o desviando correspondencia no dirigida a ellos. La pena va de 15 días a 6 meses de prisión. Si se divulga el contenido, la pena aumenta a 1 año. Si el delito es cometido por un funcionario público que abusa de sus funciones, enfrenta además una inhabilitación especial por el doble del tiempo de la condena (Código Penal de la Nación Argentina, 1984, pág. 82).

La legislación argentina relacionada con el carding establece medidas específicas para abordar la intrusión indebida en comunicaciones electrónicas y documentos privados. Con penas que varían desde 15 días hasta 6 meses de prisión, y posiblemente 1 año en caso de divulgación, se centra en salvaguardar la privacidad y la seguridad de la información digital.

Además, la incorporación de sanciones adicionales, como la inhabilitación especial para funcionarios públicos que abusen de sus funciones, refleja el compromiso de Argentina en la lucha contra el acceso no autorizado y la divulgación indebida de datos.

Es importante mencionar que los siguientes artículos, que vienen a continuación del artículo antes citado, también estipulan sanciones específicas dependiendo del agravante de la persona que cometiese un delito de carding.

En México, de acuerdo con el Código Penal Federal (en adelante CPF), con respecto al carding, manifiesta en el Capítulo IX, titulado *"Acceso ilícito a sistemas y equipos de informática*", lo siguiente:

> En el artículo 211 bis 1 compartido del Código Penal Federal (2018), se establecen penalidades para acciones no autorizadas relacionadas con la modificación, destrucción o pérdida de información en sistemas o equipos de informática protegidos por mecanismos de seguridad. Las sanciones varían de seis meses a dos años de prisión y de cien a trescientos días multa, dependiendo de la naturaleza de la infracción. (pág. 50)
>
> Por otra parte, el Art. 211 bis 2 aborda acciones similares, pero específicamente en sistemas o equipos de informática del Estado, también protegidos por mecanismos de seguridad. Las penalidades en este caso son más severas, con condenas que van de uno a cuatro años de prisión y de doscientos a seiscientos días multa. (Código Penal Federal , 2018, pág. 51)
>
> El bis tercero del Art. 211 se enfoca en la obtención, copia o uso no autorizado de información en sistemas, equipos o medios de almacenamiento informáticos de seguridad pública. Las penas varían de cuatro a diez años de prisión y multas de quinientos a mil días de salario mínimo, con medidas adicionales, como destitución e inhabilitación para servidores públicos de instituciones de seguridad pública. (Código Penal Federal , 2018, pág. 51)

Asimismo, el Art. 211 en su bis 4 trata sobre "acciones no autorizadas en sistemas o equipos de informática de instituciones financieras, con sanciones que oscilan entre seis meses y cuatro años de prisión y de cien a seiscientos días multa" (Código Penal Federal , 2018, pág. 51).

> El su bis quinto del mismo artículo, similar al tercero, se centra en acciones no autorizadas en sistemas o equipos de informática de instituciones financieras, pero con penalidades específicas para funcionarios o empleados de dichas instituciones. Las penas se incrementan en una mitad en estos casos, destacando la gravedad de las acciones cometidas por personas vinculadas a las instituciones financieras. (Código Penal Federal , 2018, pág. 51)

En resumen, los artículos establecen sanciones para la manipulación no autorizada de información en sistemas informáticos, diferenciando entre acciones en sistemas del Estado, de seguridad pública y de instituciones financieras, así como considerando la condición de autorización del perpetrador en algunos casos.

Para los efectos de los artículos 211 Bis 4 y 211 Bis 5 anteriores, se entiende por instituciones que integran el sistema financiero, las señaladas en el artículo 400 Bis de este Código. (Art. 211 bis 6)

Las penas previstas en este capítulo se aumentarán hasta en una mitad cuando la información obtenida se utilice en provecho propio o ajeno (Art. 211 bis 7)

Como último punto, las sanciones establecidas en el Código Penal Colombiano (2009), se estipulan en su Capítulo I, titulado *"De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos*" que:

> Art. 269.- ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, 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" (pág. 123)

La legislación colombiana, en el Código Penal establece sanciones para el carding bajo el artículo 269. Este artículo penaliza el acceso no autorizado a sistemas informáticos con penas de prisión de cuarenta y ocho (48) a noventa y seis (96) meses, junto con multas de 100 a 1000 salarios mínimos legales mensuales vigentes. Estas disposiciones reflejan la postura firme de Colombia contra actividades ilícitas relacionadas con el carding.

En conclusión, la proliferación de actividades delictivas en el ámbito cibernético, como el carding, ha suscitado una atención internacional creciente para establecer sanciones efectivas. Organismos como la Unión Internacional de Telecomunicaciones (UIT), la Unión Europea (UE) y la Organización de los Estados Americanos (OEA), coordinan esfuerzos para fortalecer la ciberseguridad a nivel global, con Argentina, México y Colombia destacando como líderes en la implementación de políticas y estrategias en este ámbito.

La legislación nacional de estos países, reflejada en el Código Penal Argentino, el Código Penal Federal Mexicano y el Código Penal Colombiano, establece penas específicas para el carding, manifestando una postura unificada y firme contra las prácticas ilícitas relacionadas con el acceso no autorizado y la manipulación indebida de datos en el ciberespacio.

Ante lo anteriormente expuesto, se puede concluir que este tipo de delito implica el uso indebido de información electrónica para obtener beneficios ilegítimos a expensas de la víctima. Se destacan diversas técnicas utilizadas en la comisión de este delito, como el phishing, el malware, el pharming y la ingeniería social.

Además, se abordan las respuestas legales frente a los casos de apropiación fraudulenta por medios electrónicos, incluyendo la estructura del sistema judicial en Ecuador y las medidas de protección para garantizar los derechos de las víctimas afectadas. En resumen, la legislación internacional y nacional están enfocadas en combatir los delitos cibernéticos, como el carding, mediante la implementación de medidas legales y sanciones específicas para proteger la integridad y seguridad de la información en el ciberespacio.

Metodología del Proceso de Investigación

Enfoque de la Investigación

En el marco de la evolución tecnológica y el crecimiento exponencial de las transacciones electrónicas, surge la necesidad de abordar de manera integral el delito de apropiación fraudulenta por medios electrónicos, especialmente en el entorno del sistema bancario. Este estudio cualitativo se propone analizar en profundidad las características y modalidades de este delito durante el periodo 2022-2023, centrándose de manera específica en los efectos jurídicos derivados de la violación de derechos constitucionales.

Con un enfoque cualitativo, la investigación empleará una combinación de revisión bibliográfica, análisis de casos judiciales, entrevistas con expertos legales y en seguridad informática, así como el examen detallado de legislación y jurisprudencia pertinente. Se busca comprender las tácticas utilizadas por los perpetradores, evaluar las implicaciones jurídicas y constitucionales, y, en última instancia, proporcionar recomendaciones que fortalezcan el marco legal y las medidas de seguridad en la prevención y enfrentamiento de la apropiación fraudulenta por medios electrónicos en el ámbito bancario.

> La investigación cualitativa se enfoca en el análisis de la calidad de diversas actividades, relaciones, asuntos, medios, materiales o instrumentos dentro de una situación o problema específico. Su objetivo principal es lograr una descripción holística, es decir, busca analizar de manera exhaustiva y detallada un tema o actividad en particular. A diferencia de los estudios descriptivos, correlacionales o experimentales, la investigación cualitativa no se centra principalmente en determinar las relaciones de causa y efecto entre variables. Más bien, su interés principal radica

> en comprender la dinámica y el proceso mediante el cual se desarrolla un asunto o problema en particular (Vera, 2015, p. 1).

Alcance de la Investigación

La investigación propuesta adopta un alcance exploratorio y explicativo con el fin de abordar de manera integral el delito de apropiación fraudulenta por medios electrónicos en el sistema bancario. En el alcance exploratorio, se busca adquirir un entendimiento inicial del fenómeno delictivo, explorando sus características y modalidades mediante la revisión bibliográfica y el análisis de casos judiciales.

> Estas investigaciones buscan ofrecer una visión panorámica de manera aproximada acerca de una realidad específica. Se llevan a cabo principalmente cuando el tema seleccionado ha recibido escasa exploración y reconocimiento, y aún resulta difícil formular hipótesis precisas o de alcance general, dado que se encuentra en una etapa inicial de estudio (García, 2015, p. 5).

Posteriormente, la investigación evoluciona hacia un alcance explicativa, donde se emplearán entrevistas con expertos legales y especialistas en seguridad informática. Este enfoque permitirá una comprensión más profunda de las tácticas utilizadas por los perpetradores, así como una evaluación detallada de las implicaciones jurídicas y constitucionales asociadas al delito.

De acuerdo a lo afirmado por Hernández (2006) determina que:

> Las investigaciones de carácter explicativo trascienden la mera descripción de conceptos o fenómenos, así como el establecimiento de relaciones entre ellos. Su objetivo principal consiste en abordar las causas subyacentes de eventos físicos o sociales. Como su denominación sugiere, estas investigaciones se centran en proporcionar explicaciones acerca de por qué se produce un fenómeno y en qué condiciones se manifiesta, así como en dilucidar las razones que vinculan dos o más variables entre sí (p. 66)

La combinación de métodos cualitativos establecerá un marco sólido para analizar tanto los aspectos superficiales como los subyacentes del delito de apropiación fraudulenta por medios electrónicos en el ámbito bancario, proporcionando así una base integral para futuras investigaciones y contribuyendo al fortalecimiento de medidas legales y de seguridad en la prevención y enfrentamiento de este fenómeno delictivo.

Delimitación de la Investigación

Esta investigación se llevará a cabo en Guayaquil, Ecuador, durante el periodo comprendido entre 2022 y 2023. Este marco temporal y geográfico proporcionará un contexto

específico para el análisis detallado de este fenómeno delictivo en el ámbito bancario, así como evaluar las consecuencias jurídicas relacionadas con la violación de los derechos constitucionales durante este intervalo de tiempo en dicha localidad.

Población y Muestra de la Investigación

El universo de esta investigación se extiende a individuos afectados, entidades financieras y sistemas electrónicos en el ámbito bancario de Guayaquil durante 2022-2023. Además, se incluirán abogados, jueces y fiscales especializados en el delito de apropiación fraudulenta por medios electrónicos, quienes aportarán perspectivas legales y conocimientos expertos para comprender las dinámicas y efectos jurídicos asociados con la violación de derechos constitucionales en este contexto específico.

De acuerdo a los afirmado por Pineda (1986):

> La población o universo puede abarcar diversas entidades como individuos, animales, registros médicos, datos de nacimientos, muestras de laboratorio o incluso eventos como accidentes viales. Este conjunto de elementos constituye el grupo al que se extenderán las conclusiones del estudio. Por tanto, resulta crucial identificar de manera precisa la población desde el inicio de la investigación, siendo específicos al incluir sus componentes, para garantizar la validez y relevancia de los hallazgos (p. 108).

La muestra para esta investigación estará compuesta por profesionales altamente especializados en el ámbito legal, específicamente abogados, jueces y fiscales con experiencia significativa en delitos relacionados con apropiación fraudulenta por medios electrónicos en el sistema bancario. La inclusión de profesionales del derecho garantizará una comprensión precisa y experta de los aspectos legales involucrados en el fenómeno delictivo en estudio.

> Se trata de una porción o subconjunto del universo o población en la que se realizará la investigación. La obtención de la cantidad de elementos de la muestra implica el uso de procedimientos como fórmulas y lógica, entre otros aspectos que se abordarán más adelante. La muestra, por su parte, constituye una fracción representativa de la población en estudio (López, 2004, p. 2).

La investigación se centra en un universo conformado por el conjunto total de 102,709 abogados inscritos en el Foro de Abogados de la provincia del Guayas, con un margen de error del 22% y un nivel de confiabilidad del 80%. Para llevar a cabo este estudio, se seleccionó una muestra representativa de 9 abogados, en razón de obtener las respuestas mediante profesionales del Derecho especializados en la materia.

Métodos y Técnicas de Investigación

Método Empírico

El método empírico fue empleado en la investigación debido a su capacidad para recopilar datos directos y observacionales relevantes. Esta metodología permite analizar casos judiciales, informes policiales, registros bancarios y entrevistas con víctimas y perpetradores, proporcionando una comprensión profunda de la naturaleza del delito, sus patrones de ocurrencia y sus impactos legales y sociales. Se centró en datos empíricos, lo que facilitó la identificación de tendencias, factores de riesgo y la evaluación de medidas de prevención y aplicación de la ley.

Según lo expresado por Cobas, Romeu & Macías (2010) respecto al método empírico:

> Revelan y explican las características fenomenológicas del objeto, siendo esenciales principalmente en la fase inicial de recopilación de datos empíricos y en la tercera etapa destinada a la verificación experimental de la hipótesis de trabajo. Los métodos teóricos engloban una variedad de procedimientos que facilitan la comprensión teórica de la realidad (p. 6).

En resumen, el método empírico se utilizó en este estudio porque ofrece una aproximación rigurosa y basada en evidencia para abordar un problema complejo y actual como lo es el delito de apropiación fraudulenta.

Entrevista

Se empleará la entrevista como técnica de investigación para abordar el tema propuesto. Mediante ella, se buscará obtener información directa y detallada de profesionales del derecho especializados en el delito de apropiación fraudulenta por medios electrónicos en el sistema bancario. La entrevista permitirá explorar sus perspectivas, conocimientos y experiencias, contribuyendo así a una comprensión más profunda de las características, modalidades y efectos jurídicos asociados a este fenómeno delictivo.

Al valorar la entrevista como técnica fundamental para extraer y generar conocimiento, su lógica reside en:

> Proporcionar al investigador la capacidad de comprender lo que ocurre con su objeto de estudio mediante una interpretación ilustrada. En consecuencia, su objetivo no radica en verificar el conocimiento, sino en descubrir e interpretar, a partir de diversas perspectivas, las múltiples dimensiones que conforman dicho conocimiento (Gónzalez, 2007, p. 3)

En conclusión, la obtención de información directa y detallada de profesionales del derecho especializados en este ámbito promete ofrecer una visión rica y contextualizada de las complejidades legales vinculadas a este fenómeno. La exploración de sus perspectivas, conocimientos y experiencias se traducirá en una contribución significativa para una comprensión más profunda de las características y efectos jurídicos asociados.

Procesamiento y Análisis de la Investigación

El análisis y procesamiento de resultados de la investigación sobre el delito de apropiación fraudulenta por medios electrónicos en el sistema bancario y sus implicaciones jurídicas en la violación de derechos constitucionales se llevará a cabo mediante entrevistas a profesionales del derecho especializados en el tema. Las opiniones recopiladas se tabularán y presentarán de manera resumida en tablas para su posterior análisis.

Del mismo modo, se destaca la importancia de interpretar los resultados obtenidos a la luz de la literatura existente sobre delitos financieros y tecnológicos. Se realizará un análisis detallado de los datos recopilados, destacando aspectos como la sofisticación de las técnicas utilizadas por los perpetradores, las vulnerabilidades del sistema bancario y las implicaciones legales para las víctimas.

Se espera identificar tendencias y patrones de comportamiento de los denominados carders al obtener información de tarjetas de débito o crédito para robar los fondos de sus dueños, así como las consecuencias que esto genera en la persona afectada. Además, se discutirá cómo estos actos ponen en vulneración el sistema jurídico, que hasta cierto punto no respalda el sometimiento de tales acciones.

Análisis e Interpretación de Resultados de la Investigación

Presentación de resultados

En el presente trabajo de investigación se evaluarán las consecuencias legales de los delitos financieros dentro de la industria bancaria ecuatoriana mediante consultas con especialistas en derecho penal y constitucional. El objetivo es brindar una idea clara de cómo estos delitos se relacionan con la legislación nacional, teniendo en cuenta las leyes, normas y precedentes relacionados. Además, se examinarán ciertas medidas estratégicas a fin de mejorar la seguridad del sector bancario y garantizar la integridad del marco legal. Este análisis busca ofrecer una visión amplia del problema, contribuyendo al debate académico y brindando orientación para futuras acciones legales sobre la materia.

Tabla 1

Entrevistado 1: Héctor Medina Rodríguez; Formación académica: Abogado; Cargos desempeñados: Procurador Judicial Banco Diners, Procurador Judicial Banco Machala, Abogado en libre ejercicio.

Nro.	Preguntas	Respuestas
1	**Desde su experiencia profesional, ¿cuáles son los desafíos más significativos que enfrentan los fiscales en la investigación y acusación de casos relacionados con la apropiación fraudulenta por medios electrónicos en el ámbito del sistema bancario?**	El desafío más grande que enfrentan los fiscales en este tipo de procesos, es en primer lugar, no contar con los recursos, tecnología y medios necesarios para llevar a cabo este tipo de investigaciones; en segundo lugar, no contar con el tiempo suficiente que ameritan estas investigaciones, puesto que existen demasiados procesos asignados a un solo fiscal; en tercer lugar, no contar con el conocimiento suficiente y la capacitación necesaria por parte de la Fiscalía y/o Consejo de la Judicatura para realizar este tipo de investigaciones, factores que conllevan a una negligente investigación que concluye en impunidad.
2	**¿Cuáles serían los derechos constitucionales vulnerados derivados de los casos de apropiación fraudulenta por medios electrónicos?**	El derecho a la protección de datos de carácter personal. El derecho a la intimidad personal y familiar. El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual. El derecho a la propiedad en todas sus formas.

3	**Según su opinión ¿Cuáles serían las medidas legales más efectivas para abordar y prevenir el delito de apropiación fraudulenta por medios electrónicos en el ámbito bancario?**	La imposición de nuevas obligaciones a los bancos respecto de nuevas y mejores medidas de seguridad que beneficien a sus usuarios, así como la obligación legal de los bancos de capacitar a sus clientes respecto a la ciberseguridad.
4	**¿Cuál es su punto de vista respecto al rápido avance tecnológico que ha influido en la interpretación y aplicación de las leyes sobre apropiación fraudulenta por medios electrónicos?**	Es algo normal, pues con el rápido avance tecnológico que existe, nacen también nuevas formas de delinquir a través de estos medios, pues los delincuentes también se están innovando constantemente y capacitando al respecto, existiendo la necesidad de que la legislación vaya a la vanguardia de prevenir este tipo de delitos que se puedan cometer por medios electrónicos.
5	**¿Cómo evalúa la complejidad legal al abordar y tipificar el delito de carding en Ecuador, específicamente en relación con la seguridad jurídica del usuario?**	Es un tema bastante complejo, pues de por sí es un delito que requiere cierto conocimiento técnico que nuestros legisladores no tienen, desde ahí la dificultad legal de poder no solo tipificarlo y sancionarlo, sino también crear normativa de prevención de este delito, teniendo en cuenta al usuario.
6	**¿Cuáles son las implicaciones específicas de la adición del delito de carding en la reforma del COIP en relación con la apropiación fraudulenta por medios electrónicos a través del sistema bancario?**	Considero que la inclusión de este delito en el COIP permite delimitar aún más las investigaciones penales, diferenciándolo de otros delitos que se cometen por medios electrónicos, lo cual evidentemente es positivo, pues busca atacar a un delincuente específico.

Elaborado por: Torres, E. & España, I. (2024).

Tabla 2

Entrevistado 2: Moises Haz Romero; Formación académica: Abogado; Cargos desempeñados: Especialista Jurídico del Banco Produbanco, Asistente Legal y Consultor Legal.

Nro.	Preguntas	Respuestas
1	**Desde su experiencia profesional, ¿cuáles son los desafíos más significativos que enfrentan los fiscales en la investigación y acusación de casos relacionados con la apropiación fraudulenta por medios electrónicos en el ámbito del sistema bancario?**	Existen desafíos tanto para los fiscales como para los profesionales del derecho para solidificar una teoría del caso tales como: Evidencia digital: En este primer desafío es fundamental que el Departamento de Criminalística de la Policía Judicial cuente con peritos técnicos informáticos, capaces de lograr identificar la identidad de la persona que está detrás del Skimming o del Phishing

		o del Malware, quienes son los percutores del robo de la información financiera. La falta de tipificación específica: Hoy en día existen una variedad de mutaciones de delitos, especialmente los que tienen relación con el robo de datos, de información personal y financiera. Es entonces que se debe implementar una normativa amplia que permita tipificar cada una de las conductas relacionadas con las modalidades de apropiación fraudulenta por medios electrónicos. Otro asunto es la cooperación internacional: Muchos de los ataques cibernéticos o robo de información provienen de personas que están al otro lado del mundo. Como saben los hackers operan desde cualquier parte del mundo sólo teniendo acceso a internet. Entonces la investigación de este tipo de delitos a menudo requiere de la cooperación internacional, ya que los delincuentes pueden operar desde diferentes países.
2	**¿Cuáles serían los derechos constitucionales vulnerados derivados de los casos de apropiación fraudulenta por medios electrónicos?**	Como principal derecho vulnerado siempre va ser el derecho a la propiedad privada, pues estos delincuentes deterioran el patrimonio de su víctima. El otro derecho es el de la privacidad, pues todos tenemos el derecho a mantener nuestros datos bajo reserva y que no sean divulgados por nadie, pero desde el momento que se produce un acceso no autorizado a nuestra información personal o financiera, exponemos nuestra vida, como una radiografía abierta al público.
3	**Según su opinión ¿Cuáles serían las medidas legales más efectivas para abordar y prevenir el delito de apropiación fraudulenta por medios electrónicos en el ámbito bancario?**	No creo que existan medidas efectivas para erradicar, pero sí para prevenir, y principalmente siempre va ser la educación financiera. Esta educación financiera para los clientes de la Banca, que les recuerda generalmente que el banco no solicita claves por teléfono o que tengan cuidados con correos de phishing u otras soluciones similares que prevengan a los clientes a no caer en manos de ciberdelincuentes. De allí tienes otras aristas tales como: El fortalecimiento del delito de apropiación fraudulenta por medios electrónicos incluyendo el carding. Tienes también que capacitar a fiscales sobre este tipo de delitos y la manera en que operan los ciberdelincuentes; buscar la manera de mejorar la cooperación internacional, que se necesita convenios bilaterales para el intercambio ágil de información.

4	**¿Cuál es su punto de vista respecto al rápido avance tecnológico que ha influido en la interpretación y aplicación de las leyes sobre apropiación fraudulenta por medios electrónicos?**	El rápido avance tecnológico presenta un desafío constante para la interpretación y aplicación de las leyes sobre apropiación fraudulenta por medios electrónicos. Las leyes deben ser lo suficientemente flexibles para adaptarse a las nuevas modalidades de delito que surgen con la tecnología, sin perder su eficacia en la protección de los derechos de las personas Por ejemplo, hoy en día a través de la Inteligencia artificial, ya se puede crear un avatar que se vea y escuche igual que el usuario, lo cual es un grave problema, ya que algún ciberdelincuente puede usar eso para comunicarte con un familiar tuyo, inventar una emergencia para pedir dinero y decrecer el patrimonio de tu familiar. Entonces necesitamos crear leyes con una prospectiva futurística que realmente está más cerca de llegar.
5	**¿Cómo evalúa la complejidad legal al abordar y tipificar el delito de carding en Ecuador, específicamente en relación con la seguridad jurídica del usuario?**	Empecemos por mencionar que en Ecuador no existe el tipo penal carding. Pienso que primero debemos tipificar, establecer su marco normativo protector y encontrar un equilibrio entre la necesidad de proteger a los usuarios de este tipo de ataques y el respeto a su seguridad jurídica. Esto porque si no tienes un robusto marco normativo protector, vas a ocasionar un debilitamiento en la confianza del sistema financiero y afectas a la economía digital. Recordemos que entre las cosas positivas que hubo en la pandemia del 2020, fue que hubo un alto incremento en el uso de los sistemas bancarios digitales, se aumentó el uso del dinero electrónico, de las billeteras electrónicas y así.
6	**¿Cuáles son las implicaciones específicas de la adición del delito de carding en la reforma del COIP en relación con la apropiación fraudulenta por medios electrónicos a través del sistema bancario?**	Tipificar el carding en Ecuador a través de una reforma del COIP implica un avance trascendental para el Ecuador. Asimismo, ayuda a fortalecer y robustecer al sistema financiero, al consumidor, al usuario bancario, a los negocios pequeños y pymes, en general, tiene un impacto positivo porque nos estamos alineando a proteger a la sociedad. Así por ejemplo, en el Código Penal anterior al COIP no era considerado los delitos ambientales, estos se sancionarán con multa o a veces con nada, pero el COIP trajo consigo la protección a la Pacha Mama, entonces hoy se respeta la explotación de los recursos ambientales y se contamina menos, y eso ha creado conciencia ambiental a la sociedad. Y es eso, lo que se puede lograr

		incluyendo el carding como un tipo penal sancionado por el Estado.

Elaborado por: Torres, E. & España, I. (2024).

Tabla 3

Entrevistado 3: Andrea Silva Sierra; Formación académica: Abogada; Cargos que desempeña: Abogada Asociada en Vivanco & Vivanco.

Nro.	Preguntas	Respuestas
1	**Desde su experiencia profesional, ¿cuáles son los desafíos más significativos que enfrentan los fiscales en la investigación y acusación de casos relacionados con la apropiación fraudulenta por medios electrónicos en el ámbito del sistema bancario?**	Uno de los desafíos más grandes que tiene la Fiscalía es poder individualizar al sujeto que comete la infracción y no tener a quien imputar el cometimiento del hecho punible, es decir no se puede determinar el posible autor o cómplice del acto ilícito. Adicional otro de los desafíos es la falta de conocimiento y de formación de los Fiscales para poder determinar cual es el tipo penal con el que se debe llevar a cabo el proceso. También puede ser difícil el acceso a pruebas que demuestren la fraudulencia de las conductas perpetradas, además de que muchos medios electrónicos tienen la opción de editar o borrar, por lo que es difícil encontrar las pruebas en su estado original.
2	**¿Cuáles serían los derechos constitucionales vulnerados derivados de los casos de apropiación fraudulenta por medios electrónicos?**	Entre los derechos constitucionales que se ven vulnerados por el cometimiento de estos actos delictivos tenemos que se viola el derecho a la identidad, derecho a la propiedad y los derechos del consumidor.
3	**Según su opinión ¿Cuáles serían las medidas legales más efectivas para abordar y prevenir el delito de apropiación fraudulenta por medios electrónicos en el ámbito bancario?**	Fortalecer las capacidades de investigación y persecución de delitos cibernéticos por parte de las autoridades competentes. Esto implica la asignación de recursos adecuados, la capacitación de personal especializado y la cooperación internacional en casos transfronterizos. Fomentar la colaboración entre entidades financieras, autoridades gubernamentales y organismos de seguridad para intercambiar información sobre amenazas cibernéticas y desarrollar estrategias conjuntas de prevención y respuesta.
4	**¿Cuál es su punto de vista respecto al rápido avance tecnológico que ha influido en la interpretación y aplicación de las leyes sobre apropiación fraudulenta por medios electrónicos?**	Actualmente estamos en una generación tecnológica entonces es común que todo vaya avanzando, las personas van evolucionando con el tiempo y con eso la tecnología, por lo que hay que implementar medidas de seguridad para que la tecnología siempre sea de aporte y no cause perjuicio, ya que al final quienes cometen el perjuicio son las

		personas. Es parte de la evolución tecnológica que vive el mundo hoy en día, por ello, al mismo tiempo deben evolucionar las leyes que protejan los bienes jurídicos vulnerados.
5	**¿Cómo evalúa la complejidad legal al abordar y tipificar el delito de carding en Ecuador, específicamente en relación con la seguridad jurídica del usuario?**	En lo personal además de la complicación que se tiene al momento querer castigar a los infractores con el delito tipificado en el artículo 190 del COIP, se podría desarrollar más incisos dentro del artículo antes mencionado para que así cubra todo tipo de modalidades que puede realizar un ciberdelincuente o en su defecto debido a la complejidad que amerita el carding ésta debería estar tipificada como un delito autónomo ya que eso permitiría el correcto desarrollo de la seguridad jurídica en este tipo de actos delictivos.
6	**¿Cuáles son las implicaciones específicas de la adición del delito de carding en la reforma del COIP en relación con la apropiación fraudulenta por medios electrónicos a través del sistema bancario?**	La inclusión del delito de carding en la reforma del COIP fortalece el marco legal para abordar el uso fraudulento de información de tarjetas en línea, permite imponer sanciones más severas, fomenta la cooperación internacional en investigaciones y asigna recursos adicionales para combatir este tipo de delitos.

Elaborado por: Torres, E. & España, I. (2024).

Tabla 4

Entrevistado 4: Edgar Exer Zambrano Ramirez; Formación académica: Abogado; Cargo que desempeña: Libre ejercicio.

Nro.	Preguntas	Respuestas
1	**Desde su experiencia profesional, ¿cuáles son los desafíos más significativos que enfrentan los fiscales en la investigación y acusación de casos relacionados con la apropiación fraudulenta por medios electrónicos en el ámbito del sistema bancario?**	Entre los desafíos más significativos que tenemos es quizás el desconocimiento de la figura como tal para poderla relacionar a un tipo penal establecido en el Ecuador, para que dicho cometimiento del delito pueda ser castigado, esto se debe a la falta de capacitaciones que tienen los Fiscales en cuanto al cometimiento de delitos electrónicos. Adicionalmente otro de los desafíos al que se enfrentan los fiscales es determinar el tema de la territorialidad, en virtud de que esta pudo haberse ejecutado fuera de la jurisdicción nacional sin poder identificar verdaderamente al sospechoso.
2	**¿Cuáles serían los derechos constitucionales vulnerados derivados de los casos de apropiación fraudulenta por medios electrónicos?**	Desde mi perspectiva los derechos vulnerados son: el derecho a la propiedad privada, el derecho a la protección de datos, el derecho a la privacidad.

3	**Según su opinión ¿Cuáles serían las medidas legales más efectivas para abordar y prevenir el delito de apropiación fraudulenta por medios electrónicos en el ámbito bancario?**	Entre las medidas que se podrían implementar sería que se le otorgue a la Fiscalía un manual, el cual le describa las diversas modalidades para cometer delitos cibernéticos, para que así se puedan alinear a los tipos penales que están contemplados en el Código Orgánico Integral Penal. Adicional considero que también se deberían implementar medidas de seguridad informática modernas alineadas con inteligencia artificial que pueda detectar todo tipo de amenaza externa.
4	**¿Cuál es su punto de vista respecto al rápido avance tecnológico que ha influido en la interpretación y aplicación de las leyes sobre apropiación fraudulenta por medios electrónicos?**	Al estar en un mundo totalmente globalizado y sobre todo al alcance de la tecnología para cualquier persona, no es menos cierto que el derecho tiene que caminar al mismo tiempo, y más aún el derecho penal que protege los bienes jurídicos protegidos por la ley. En un mundo cada vez más interconectado, el derecho penal debe estar acorde para enfrentar, adaptarse y garantizar la protección efectiva de los derechos de las personas, lo cual no está sucediendo con el artículo 190 del COIP, el cual debería ser reformado para abarcar la problemática actual.
5	**¿Cómo evalúa la complejidad legal al abordar y tipificar el delito de carding en Ecuador, específicamente en relación con la seguridad jurídica del usuario?**	Creo que no existe una preponderancia para que se tipifique el delito de carding como autónomo; sin embargo, estoy de acuerdo que dependiendo de las circunstancias en la que se comete ésta conducta, se pueda agregar estos comportamientos de los ciberdelincuentes dentro de los tipos penales ya establecidos, es decir que pueda adecuarse la norma actual a las diferentes modalidades de estos delitos agregando nuevos incisos, por lo cual no existiría ningún tipo de complejidad al tipificar ya que lo que se haría es una expansión de la norma ya existente.
6	**¿Cuáles son las implicaciones específicas de la adición del delito de carding en la reforma del COIP en relación con la apropiación fraudulenta por medios electrónicos a través del sistema bancario?**	Las implicaciones por el cometimiento de cualquier delito, en este caso un delito financiero, es la rigidez que debe tener en cuanto a la aplicación de penas y beneficios procesales y penitenciarios. Es de suma importancia que al implementar este tipo de comportamientos delictuosos, se establezcan las medidas necesarias para garantizar la efectividad y la protección de los derechos de los usuarios.

Elaborado por: Torres, E. & España, I. (2024).

Tabla 5

Entrevistado 5: Arnaldo Alfonso Idrovo Gonzales; Formación académica: Abogado; Cargos que desempeña: Comisario de Policía, Abogado en libre ejercicio.

Nro.	Preguntas	Respuestas
1	**Desde su experiencia profesional, ¿cuáles son los desafíos más significativos que enfrentan los fiscales en la investigación y acusación de casos relacionados con la apropiación fraudulenta por medios electrónicos en el ámbito del sistema bancario?**	Dentro de los desafíos que suelen enfrentar los Fiscales en estos tipos de delitos informáticos,es que en muchas ocasiones no se puede determinar a la persona que comete el delito, debido a su naturaleza no se puede determinar quien es la persona que está obteniendo la información, desde dónde se obtiene la información, en algunas ocasiones este delito ni siquiera es cometido dentro del territorio nacional, sino que son personas desde el exterior.
2	**¿Cuáles serían los derechos constitucionales vulnerados derivados de los casos de apropiación fraudulenta por medios electrónicos?**	En mi opinión, los derechos que se ven afectados son el derecho a la propiedad privada, el derecho a la protección de la información personal y el derecho a la intimidad.
3	**Según su opinión ¿Cuáles serían las medidas legales más efectivas para abordar y prevenir el delito de apropiación fraudulenta por medios electrónicos en el ámbito bancario?**	Una de las medidas legales que se podrían implementar para poder abordar el delito de apropiación fraudulenta por medios electrónicos es ampliarlo o reformarlo a lo que nos queremos referir en los diversos modos de cometer el delito e indicar a través de cuales medios se puede cometer. Con respecto a la prevención de dicho delito estaría la implementación de algún tipo de instructivo que se ponga en conocimiento de las autoridades ya que en muchas ocasiones al ser delitos informáticos no cuentan con el conocimiento técnico respecto a la tecnología que pueden usar los ciberdelincuentes.
4	**¿Cuál es su punto de vista respecto al rápido avance tecnológico que ha influido en la interpretación y aplicación de las leyes sobre apropiación fraudulenta por medios electrónicos?**	En la actualidad es normal el avance tecnológico y conforme dicho avance también hay un avance en los delitos; por eso creo que, lo que debemos hacer actualmente es adaptar las normas penales que ya se encuentran establecidas, en este caso el artículo 190 del COIP, poderlo adaptar a esta nueva modalidad de delitos, ya que hoy en día la tecnología es un campo que da apertura para el cometimiento de nuevos delitos.
5	**¿Cómo evalúa la complejidad legal al abordar y tipificar el delito de carding en Ecuador, específicamente en relación con la seguridad jurídica del usuario?**	Personalmente no veo complejo tipificar este delito, porque como vengo diciendo, actualmente este tipo de comportamientos genera conmoción social, por lo que creo que existen diversas formas de agregar este comportamiento, la primera es que se tipifique como delito autónomo, otra sería que se agreguen más incisos abarcando la

		problemática actual o por último se podría incluir estas conductas en un artículo a continuacion del 190 del coip, como un artículo innumerado o agregar un artículo como por ejemplo ponerle un art. 190.1 o 190 A para que así se abarque todas las nuevas conductas que actualmente no están reguladas.
6	**¿Cuáles son las implicaciones específicas de la adición del delito de carding en la reforma del COIP en relación con la apropiación fraudulenta por medios electrónicos a través del sistema bancario?**	Una implicación específica sería que se estaría extendiendo el poder punitivo del estado, por lo que la justificación que yo encuentro para agregar este delito es que se quiera tener mayor visibilidad del cometimiento del mismo, entonces considero y mantengo mi punto de vista anterior que es que se agregue la conducta del carding dentro del Art. 190 como un inciso o varios incisos que contemplen esta conducta, para que así establezca todas las modalidades y pueda estar cubierto en cualquier tipo de actos delictivos.

Elaborado por: Torres, E. & España, I. (2024).

Tabla 6

Entrevistado 6: Kleber Alexis Riofrío Olaya; Formación académica: Abogado, Máster en Derecho Constitucional; Cargo que desempeña: Abogado en libre ejercicio.

Nro.	Preguntas	Respuestas
1	**Desde su experiencia profesional, ¿cuáles son los desafíos más significativos que enfrentan los fiscales en la investigación y acusación de casos relacionados con la apropiación fraudulenta por medios electrónicos en el ámbito del sistema bancario?**	En la investigación penal, la cual es la fase de recaudación de indicios y elementos de convicción, lo cual se verá reflejado en la acusación, el problema en los elementos es la técnica y el apoyo científico ya que se debe apoyar precisamente a estos tipos penales y en este tipo en específico se requiere de mucho apoyo técnico e informático, por lo cual considero que los hackers o las persona que cometen este delito por los medios electrónicos, generalmente no dejan huellas para evitar ser rastreados e identificados. Entonces, el problema es técnico, ya que esto se ve en la recaudación de los elementos de convicción y finalmente este problema se verá también en la acusación, ya que sería débil y/o flojo, la consecuencia de aquello sería que el juez emita un sobreseimiento. Esta situación se podría mejorar haciendo que el sistema de criminalística tenga mejor capacitación, tenga peritos más especializados en materia científica,

		informática y también de economía para que puedan seguir los rastros y puedan llegar a una verdad material.
2	**¿Cuáles serían los derechos constitucionales vulnerados derivados de los casos de apropiación fraudulenta por medios electrónicos?**	La Constitución reconoce la propiedad privada, el derecho a la privacidad y a la protección de datos.
3	**Según su opinión ¿Cuáles serían las medidas legales más efectivas para abordar y prevenir el delito de apropiación fraudulenta por medios electrónicos en el ámbito bancario?**	Las medidas legales más efectivas para abordar y prevenir el delito de apropiación fraudulenta, más que legales deben ser medidas técnicas científicas, que las bancas tengan un sistema informático que sea sólido, que sea seguro y así los usuarios tengan todas las precauciones del caso.
4	**¿Cuál es su punto de vista respecto al rápido avance tecnológico que ha influido en la interpretación y aplicación de las leyes sobre apropiación fraudulenta por medios electrónicos?**	El derecho va de la mano con el desarrollo de la sociedades y los pueblos, el derecho no es el mismo que era hace 20, 40 o 60 años y esto es porque la sociedad ya no es la misma; las sociedades han cambiado con los avances tecnológicos y precisamente esos avances tecnológicos deben de ser reglados, enmarcados, para que exista una correcta armonía y para que se precautela y se le dé seguridad a los bienes jurídicos protegidos que se ven inmersos en este transitar tecnológicos.
5	**¿Cómo evalúa la complejidad legal al abordar y tipificar el delito de carding en Ecuador, específicamente en relación con la seguridad jurídica del usuario?**	No veo ningún tipo de complejidad para que se tipifique el carding, ya que respecto a este delito que se conoce que es una modalidad que afecta el patrimonio de las personas, efectivamente se debe tipificar para así asegurar la vigencia de la seguridad jurídica, no sólo para la víctima sino también para el investigado.
6	**¿Cuáles son las implicaciones específicas de la adición del delito de carding en la reforma del COIP en relación con la apropiación fraudulenta por medios electrónicos a través del sistema bancario?**	Las implicaciones específicas de la adición del delito, es conveniente porque una vez que esté tipificado se puede iniciar investigaciones y se puede iniciar procesos por aquel delito que es una modalidad de conducta, que actualmente no se encuentra tipificado. Debemos recordar que por el principio de interpretación penal, son establecidas en el Artículo 13 COIP y además por el principio de seguridad jurídica y los principios penales clásicos, nadie puede ser juzgado y/o sancionado por un delito y/o una conducta que no haya sido tipificada.

Elaborado por: Torres, E. & España, I. (2024).

Tabla 7

Entrevistado 7: José Ignacio Arevalo Santana; Formación académica: Abogado; Cargos que desempeña: Asesor Jurídico en la Federación Deportiva Nacional del Ecuador, miembro de asesoría jurídica en el consejo electoral del Guayas.

Nro.	Preguntas	Respuestas
1	**Desde su experiencia profesional, ¿cuáles son los desafíos más significativos que enfrentan los fiscales en la investigación y acusación de casos relacionados con la apropiación fraudulenta por medios electrónicos en el ámbito del sistema bancario?**	Entre los desafíos más significativos tenemos la falta de experticia y de un laboratorio en el área de criminalística a fin de desarrollar elementos complementarios para determinar el esclarecimiento de esos hechos, esta carencia en muchas ocasiones ha impedido que se puedan recolectar pruebas contundentes para poder dar con los implicados del acto delictivo, dejando así muchos delitos en la impunidad. Adicional tenemos el hecho que en muchas ocasiones como la ley penal es taxativa y los ciberdelincuentes utilizan técnicas, métodos o medios que no están tipificados por nuestra legislación a los mismos no se les puede encasillar en otros tipos de delitos.
2	**¿Cuáles serían los derechos constitucionales vulnerados derivados de los casos de apropiación fraudulenta por medios electrónicos?**	Desde mi punto de vista, los derechos que se ven comprometidos son el derecho a la propiedad privada, el derecho a la protección de datos y el derecho a la intimidad.
3	**Según su opinión ¿Cuáles serían las medidas legales más efectivas para abordar y prevenir el delito de apropiación fraudulenta por medios electrónicos en el ámbito bancario?**	Establecer una ley de protección a la vigencia de la norma, esto quiere decir que se estructure la normativa que impida primero la obtención de información y segundo una protección mucho más adecuada en el sistema electrónico y/o digital que no permita que haya acceso con tanta facilidad al mismo, lo cual determinaría que tiene que hacerse una estructura en el sistema financiero que no dependa únicamente de la banca.
4	**¿Cuál es su punto de vista respecto al rápido avance tecnológico que ha influido en la interpretación y aplicación de las leyes sobre apropiación fraudulenta por medios electrónicos?**	No hay un extenso catálogo de tipos penales para determinar y regular el comportamiento en ese ámbito, lo que existe son normativas generales acerca de la protección de datos y en función a la restricción del acceso pero no hay algo que proteja al bien jurídico como tal más allá que si bien es un derecho que se encuentra consagrado en la constitución, no existe una normativa que regule ese tipo de situaciones de bien jurídico es decir una garantía para este tipo de acciones de bien

		jurídico esto necesitaría una reforma integral también en la norma penal.
5	**¿Cómo evalúa la complejidad legal al abordar y tipificar el delito de carding en Ecuador, específicamente en relación con la seguridad jurídica del usuario?**	Determinar mayor responsabilidad en el área del sistema financiero, es decir cuando hablamos de protección de la norma jurídica o de garantías, no solo debe sancionarse a quien ejecuta la acción, sino también a quien permita en el sistema financiero que se ejecute la acción. Es decir no solamente debe establecerse un concepto de responsabilidad penal para quien ejecuta el acto de manera activa pero también debe establecerse una responsabilidad penal para quien permite. Por lo tanto, se debe tipificar la conducta que engloba el delito de Carding para así establecer penas y responsabilidades a quienes cometan y permitan el cometimiento de estos actos.
6	**¿Cuáles son las implicaciones específicas de la adición del delito de carding en la reforma del COIP en relación con la apropiación fraudulenta por medios electrónicos a través del sistema bancario?**	Incluir el delito carding como una infracción específica dentro del Artículo 190 del COIP tendría como resultado que se puedan castigar estas nuevas conductas delictivas y facilitaría su investigación lo cual permite que quienes investigan el proceso penal puedan realizar su trabajo de una mejor manera; además, serviría para resguardar a los usuarios y entidades financieras de los daños ocasionados por el carding.

Elaborado por: Torres, E. & España, I. (2024).

Tabla 8

Entrevistado 8: Erika Paola Pluas Luna; Formación académica: Abogada; Cargos que desempeña: SecretarÍa de Coactiva IESS, Abogada Externa Banco Diners Club S.A

Nro.	Preguntas	Respuestas
1	**Desde su experiencia profesional, ¿cuáles son los desafíos más significativos que enfrentan los fiscales en la investigación y acusación de casos relacionados con la apropiación fraudulenta por medios electrónicos en el ámbito del sistema bancario?**	En la actualidad la inseguridad no solo afecta al ser humano per se, sino también a los diversos sistemas que debemos utilizar y que lastimosamente en nuestro País aun no están debidamente tipificados como delitos, ahora bien desde mi punto de vista los Fiscales enfrentan los siguientes desafíos: E desconocimiento de las nuevas metodologías de cometer delitos informáticos y el poco alcance de investigación y la poca tecnología a la que tiene acceso la fiscalía en comparación a los delincuentes.
2	**¿Cuáles serían los derechos constitucionales vulnerados derivados de los casos de**	Principalmente los derechos de libertad consagrado en el Art 66 de la CRE numerales 19,20 y 21.

	apropiación fraudulenta por medios electrónicos?	
3	**Según su opinión ¿Cuáles serían las medidas legales más efectivas para abordar y prevenir el delito de apropiación fraudulenta por medios electrónicos en el ámbito bancario?**	Tipificación de nuevos delitos de carácter informáticos y penas mas rigurosas con quienes infringe las mismas.Además de sanciones a las instituciones (publicas y privadas) que posean bases de datos de la ciudadanía y que luego de una investigación se constate que esta realice venta de esta información o también haya realizado lo comúnmente conocido como fuga de datos sensibles.
4	**¿Cuál es su punto de vista respecto al rápido avance tecnológico que ha influido en la interpretación y aplicación de las leyes sobre apropiación fraudulenta por medios electrónicos?**	En el país el avance tecnológico no va de la mano con las leyes con las que contamos para poder regular esta problemática, dicho de otra forma vamos 5 pasos atrás del como castigamos un delito de apropiación fraudulenta a la rapidez con la que los delincuentes lo realizan.
5	**¿Cómo evalúa la complejidad legal al abordar y tipificar el delito de carding en Ecuador, específicamente en relación con la seguridad jurídica del usuario?**	La complejidad legal en el país respecto a este tema es muy leve, se necesita rigurosidad en cuanto a las leyes y concientización en los usuarios para que sepan identificar si presentan alguna vulnerabilidad en sus datos.
6	**¿Cuáles son las implicaciones específicas de la adición del delito de carding en la reforma del COIP en relación con la apropiación fraudulenta por medios electrónicos a través del sistema bancario?**	Los efectos de la adición de un nuevo delito en el código integral penal , son cruciales para poder determinar su aplicación y alcance. Es importante comprender estos aspectos para garantizar el cumplimiento legal y la protección de las personas. Las implicaciones especificas serian principalmente en la socialización y la garantía hacia el usuario acerca de la protección y tratamiento de sus datos.

Elaborado por: Torres, E. & España, I. (2024).

Tabla 9

Entrevistado 9: Alex Javier Lopez Ávila; Formación académica: Abogado; Cargo que desempeña: Fiscal en la Provincia del Guayas.

Nro.	Preguntas	Respuestas
1	**Desde su experiencia profesional, ¿cuáles son los desafíos más significativos que enfrentan los fiscales en la investigación y acusación de casos relacionados con la apropiación fraudulenta por medios electrónicos en el ámbito del sistema bancario?**	Entre los desafíos que enfrentamos los fiscales dentro de este tipo de delitos es que no se cuenta con una buena unidad que se dedique específicamente a la investigación de estos delitos; o que, dentro de la policía exista un agente investigador que acompañe a los fiscales en estos delitos, pero para ello, la policía debe haber capacitado previamente a los policías para que hagan

		esto; sin embargo actualmente no se cuenta con esa preparación.
2	**¿Cuáles serían los derechos constitucionales vulnerados derivados de los casos de apropiación fraudulenta por medios electrónicos?**	El derecho vulnerado es la propiedad.
3	**Según su opinión ¿Cuáles serían las medidas legales más efectivas para abordar y prevenir el delito de apropiación fraudulenta por medios electrónicos en el ámbito bancario?**	Entre las medidas más efectivas que se pueden implementar para este tipo de delitos es el uso de medidas cautelares ya que una de las cosas que busca la gente siempre es la inmovilización, es decir medidas cautelares de carácter real. Lo que se necesita es que sea mucho más ágil el proceso, para eso son las medidas de carácter real que no las dispone el fiscal, ya que éstas se las solicita y las dispone el Juez.
4	**¿Cuál es su punto de vista respecto al rápido avance tecnológico que ha influido en la interpretación y aplicación de las leyes sobre apropiación fraudulenta por medios electrónicos?**	El rápido avance tecnológico es una realidad que ha influido en el cometimiento de nuevas formas de delinquir, por lo que los legisladores deben adaptar las leyes a la realidad cambiante, la legislación tiene que encontrar maneras de poder avanzar al mismo ritmo que está avanzando nuestra realidad; por lo que, en el caso que algunos delitos se estén cometiendo y ciertas conductas no se encuentren tipificadas, lo correcto sería que la ley actual se ajuste a estas nuevas modalidades.
5	**¿Cómo evalúa la complejidad legal al abordar y tipificar el delito de carding en Ecuador, específicamente en relación con la seguridad jurídica del usuario?**	Desde mi punto de vista no existe una complejidad para tipificarlo y abordarlo, ya que el tipo penal anteriormente mencionado en el articulo 190 del COIP ya contempla ciertas características; sin embargo, lo que se necesita hacer es poner un inciso adicional donde se aclaren o se tipifiquen estas nuevas conductas para que no exista confusión, para que al momento que los fiscales requieran formular cargos en contra de quienes cometen estos actos y así poder dar continuidad al proceso y no se estanque. Adicionalmente, se pueden establecer medidas de prevención dentro del ámbito administrativo.
6	**¿Cuáles son las implicaciones específicas de la adición del delito de carding en la reforma del COIP en relación con la apropiación fraudulenta por medios electrónicos a través del sistema bancario?**	Agregar el carding como un delito específico dentro del Artículo 190 del COIP tendría el efecto de aumentar la visibilidad y la gravedad de esta actividad delictiva y facilitar su enjuiciamiento y persecución, promoviendo una mayor colaboración entre las autoridades a nivel nacional e internacional. Esto ayudaría a proteger a los

		usuarios y a las instituciones financieras de los efectos perjudiciales del carding y contribuiría a la seguridad y estabilidad del sistema financiero en general.

Elaborado por: Torres, E. & España, I. (2024).

Discusión de resultados

Con relación a las nueve entrevistas realizadas a profesionales del derecho, se puede inferir que de la pregunta número uno, el 50% de ellos insiste en que la falta de recursos como tecnología y tiempo debilita significativamente la efectividad para investigar y perseguir la apropiación electrónica fraudulenta en el sector bancario. Esto se debe a que los fiscales se ven obligados a realizar investigaciones muy concluyentes, lo que también significa que no tienen libertad para implementar procedimientos judiciales eficaces. Mientras tanto, el otro 50% destacó que las pruebas digitales, la falta de una clasificación específica de los delitos y la necesidad de cooperación internacional desempeñan papeles cruciales a la hora de influir en la capacidad de los fiscales para abordar eficazmente estos casos debido a la naturaleza volátil y siempre cambiante de los medios electrónicos. Los delitos financieros deben estar respaldados por una legislación clara y adaptable.

Respecto a la segunda pregunta, se evidencia un consenso del 100% entre los entrevistados respecto al derecho a la propiedad privada como el derecho principal mas vulnerado. Esta convergencia pone de relieve la importancia de salvaguardar este derecho humano inalienable, ya que los delincuentes destruyen las propiedades de las víctimas. Igualmente importante es el derecho a la privacidad, que incluye la protección de datos personales y financieros, que también marca otro derecho esencial violado en tales casos. Enfatiza cuán desesperadamente se deben implementar tales medidas para garantizar la seguridad tanto de la propiedad privada como de la privacidad de quienes son víctimas de este tipo de delitos electrónicos.

Por otra parte, de la tercera pregunta, el 100% de los entrevistados destacaron unánimemente que es muy necesario imponer nuevas obligaciones a los bancos para mejorar los niveles de seguridad a través de la capacitación en seguridad cibernética y la educación financiera de los clientes como medida preventiva clave para advertir a los clientes sobre peligros probables. Además, se recomienda además fortalecer las capacidades de investigación y enjuiciamiento de los delitos cibernéticos mediante la asignación de recursos adecuados y el fomento de la coordinación entre las instituciones financieras, las autoridades gubernamentales y los organismos encargados de hacer cumplir la ley. Por ello, la relevancia de incorporar sistemas avanzados de seguridad informática reforzados con inteligencia artificial para proteger a los usuarios y evitar el acceso no autorizado a sus datos financieros.

Estos puntos de vista enfatizan que es necesario abordar eficazmente este fenómeno mediante medidas tanto legales como técnicas.

En cuanto a la cuarta pregunta, se puede observar que el 70% de los entrevistados abogan por la evolución de la ley en sincronía con la sociedad y la integración con la tecnología, que es un nuevo sistema de seguridad destinado a garantizar la integridad y confiabilidad de la propiedad legal. Esto implica centrarse en el desarrollo de nuevas regulaciones penales para combatir el crimen en el entorno tecnológico contemporáneo. Por otro lado, el 30% restante cree que la tecnología debería protegerse con medidas propias, ya que se puede abusar de ella y la tecnología debería verse más bien como un elemento positivo que necesita control. Las perspectivas mencionadas anteriormente revelan cómo no es fácil mantener leyes actualizadas en una era donde la tecnología cambia más rápido que nunca, lo que hace necesaria una legislación flexible para enfrentar cualquier desafío.

Asimismo al abordar la quinta pregunta, se desprende que la evaluación revela una división del 60% de los entrevistados que consideran que no existe mucha complejidad para caracterizar y considerar adecuadamente el delito de carding en el Ecuador. Estos entrevistados sugieren que es necesario definir las características esenciales del delito y esbozar precauciones específicas para garantizar la protección de los derechos y la seguridad de las transacciones financieras de las víctimas potenciales. Sin embargo, el 40% restante, previó varias formas de incluir el uso de tarjetas bancarias en el derecho penal: como un delito independiente o como uno más de los tipos existentes. Estos puntos de vista denotan la importancia de abordar la complejidad legal del carding para la protección del usuario dentro del contexto legal ecuatoriano

Finalmente, respecto a la sexta pregunta se evidencia que el 100% de los entrevistados consideran que la inclusión del delito de carding en la reforma del COIP es importante para abordar el fraude por vía electrónica dentro de un sistema bancario. Todos los encuestados piensan que esta adición mejoraría la visibilidad y la gravedad de la criminalidad, facilitaría su persecución y daría como resultado una mejor cooperación entre las instituciones nacionales e internacionales.

La adopción de estas medidas se consideran un paso crucial en la prevención de los efectos nocivos del carding, no sólo en los usuarios sino también en las instituciones financieras, mejorando así la seguridad en todo el sistema.

En definitiva, existe una necesidad apremiante, tal como lo expresaron de manera unánime los entrevistados, de incluir el delito de carding dentro del marco legal del Artículo 190 del COIP, abarcando así el espectro de los delitos financieros electrónicos. Esta incorporación se erige como un paso crucial para enfrentar de manera adecuada la creciente amenaza que representa el carding en el ámbito bancario ecuatoriano.

Al hacerlo, se mejoraría la capacidad del sistema legal para identificar, enjuiciar y sancionar a los perpetradores de este tipo de delitos, lo que a su vez fortalecería la confianza en el sistema financiero y protegería los derechos e intereses de los usuarios. Además, mediante la creación de una base legal sólida para prevenir el carding, es posible sentar un precedente para futuras medidas legales y preventivas destinadas a garantizar la ciberseguridad en la banca.

En este sentido, la propuesta que se presentará más adelante en respuesta a las preocupaciones expresadas por los entrevistados debe reflejar esta necesidad imperante, garantizando así una mayor seguridad jurídica y una protección más efectiva contra los delitos financieros electrónicos, en particular el carding, en Ecuador.

Propuesta

En el contexto actual de la creciente sofisticación de los delitos cibernéticos y la necesidad de adaptar la legislación penal a los nuevos desafíos tecnológicos, se plantea una propuesta de reforma al artículo 190 del Código Orgánico Integral Penal (COIP) en Ecuador. Esta iniciativa se basa debido a que han salido a la luz un crecimiento de los delitos con tarjetas, que ha dado origen a la tecnología y pone en riesgo la seguridad financiera y privada de los usuarios.

Al tipificar el delito de carding dentro de la propuesta de reforma es un intento de cerrar la brecha legislativa que no aborda el acto de respecto a el uso de tarjetas en sí y sus actividades y delitos relacionados en el cuerpo legal para establecer una base legal clara para la prevención y supresión de este.

Para resolver los desafíos existentes y anticipar los posibles desafíos futuros de la ciberdelincuencia, esta propuesta surge de la preocupación de garantizar la protección jurídica de las personas, así como de solidificar aún más el marco legislativo. Un intento importante en esto es categorizar el carding como un delito y establecer penas severas que puedan imponerse contra cualquiera que lo realice, de modo que se pueda saber que actos de tal naturaleza no serían aceptados de ninguna manera y se seguirían acciones estrictas para garantizar que los derechos de los usuarios y la privacidad en las plataformas digitales estén efectivamente salvaguardados.

Título de propuesta

“Proyecto de Ley reformatoria del Artículo 190 del Código Orgánico Integral Penal relativa a la protección contra delitos financieros electrónicos en el Ecuador”

Objetivo de la propuesta

Proponer la inclusión del delito de carding mediante una reforma legislativa del Art. 190 del COIP, con el fin de fortalecer la protección de los usuarios bancarios y garantizar una mayor seguridad jurídica en Ecuador.

Justificación de la propuesta

La justificación de esta propuesta surge debido la alta demanda que surge ante la manifestación emergente del delito de carding, como una amenaza a la seguridad económica y también a la protección de la identidad de los usuarios en el Ecuador. La inserción del

carding en el artículo 190 del COIP proporcionaría pautas concretas y sencillas para la investigación, el procesamiento y el castigo de este tipo de delitos, mejorando así la capacidad del sistema legal para abordar los delitos financieros electrónicos de manera más eficiente.

La carencia de una regulación específica respecto con respecto al carding, crea un vacío legal que dificulta localizar y perseguir a los sospechosos, lo que impide que las autoridades respondan de manera adecuada. Sin embargo, la promulgación de leyes claras sobre el cardado puede enviar una severa advertencia a los perpetradores de que tales actividades criminales no serán toleradas por el sistema judicial, lo que puede desalentar a los posibles delincuentes y disminuir la ocurrencia de este delito.

Además, al momento de que se garantiza que se preserven los derechos e intereses de los usuarios, la estabilidad y seguridad de las instituciones financieras contribuirían en gran medida a generar confianza en el sector bancario y a apoyar el crecimiento económico sostenible en Ecuador.

Beneficios de la propuesta

La inclusión del delito de carding en el Artículo 190 del COIP beneficiará a que muchos usuarios al momento de combatir los delitos financieros electrónicos. Para que los responsables de la investigación de tales delitos, mediante la reforma legal brindada ayude a establecer y definir criterios claros de identificación y sanción de los delincuentes, a fin de que se puedan realizar investigaciones más eficientes y efectivas, fomentando así la cooperación entre agencias gubernamentales y organismos internacionales.

De acuerdo a las autoridades judiciales, la incorporación del carding al marco legal es un gran paso adelante en la defensa de la justicia y la protección de los derechos humanos. Con estatutos específicos vigentes, los tribunales podrán manejar los casos de carding con más confianza, asegurando que los culpables reciban el castigo merecido mientras se imponen multas justificadamente.

La integración del carding al sistema legal en Ecuador es generalmente para el mejoramiento de la sociedad, ya que crea un entorno financiero más seguro. Minimizar los peligros relacionados con el uso de la banca electrónica desarrolla la confianza en el sistema bancario y también fomenta la inclusión económica, mientras que afirmar que los derechos de los ciudadanos están protegidos y los culpables deben rendir cuentas fomenta el estado de derecho y, a su vez, fomenta una sociedad justa.

Desarrollo de la propuesta

Se ha elaborado la propuesta de reforma legal que abarca el artículo 190 del Código Orgánico Integral Penal, con el propósito de abordar el delito específico del carding mediante apropiación fraudulenta por medios electrónicos. La propuesta prevée insertar un inciso que defina los actos y elementos que constituyen el delito de carding; a fin de garantizar que las fuerzas del orden comprendan mejor su aplicación y que las personas no queden impunes.

De esta forma, se pretende proporcionar medios legales adecuados tanto a los actores de la justicia como a las víctimas para que puedan someterse a un juicio justo y efectivo, garantizando que los culpables comparezcan ante la justicia.

Proyecto de ley de reformatoria del artículo 190 del Código Orgánico Integral Penal referente relativa a la protección contra los delitos financieros electrónicos en el Ecuador.

La Asamblea Nacional de la República del Ecuador

Considerando

Que el Artículo 11 de la Constitución de la República establece que ninguna norma jurídica puede limitar los derechos constitucionales, mientras que el numeral 9 destaca la obligación primordial del Estado de respetar y garantizar estos derechos.

Que el Artículo 82 de la Constitución establece que el derecho a la seguridad jurídica se basa en el respeto a la Constitución y en la existencia de normas claras, públicas y aplicadas por autoridades competentes.

En ejercicio de los deberes y atribuciones previstas en el artículo 120, numeral 6 de la Constitución de la República, en concordancia con el artículo 9, numeral 6 de la Ley Orgánica de la Función Legislativa, resuelve expedir la siguiente:

Ley de reformatoria del artículo 190 del Código Orgánico Integral Penal referente relativa a la protección contra los delitos financieros electrónicos en el Ecuador.

Artículo 1.- Agréguese al artículo 190 un segundo inciso que diga lo siguiente:

“Se considerará carding cualquier acción que implique la falsificación, copia o robo de tarjetas bancarias o información financiera, con el propósito de obtener beneficio propio o ajeno a través de la sustracción de fondos o bienes de terceros. La persona que utilice fradulentamente los sistemas informáticos o redes electrónicas para obtener de manera ilícita

información financiera, incluyendo números de tarjetas de crédito o débito, así como datos personales proporcionados en línea, con el fin de realizar transacciones no autorizadas o cometer fraude sera sancionada con una pena privativa de libertad de uno a tres años.”

Disposición Final. - Deróguense todas las disposiciones legales y reglamentarias que contravengan la presente ley, la misma que entrará en vigencia a partir de su promulgación y publicación en el Registro Oficial.

Finalmente, la iniciativa de reformar el artículo 190 del Código Orgánico Integral Penal (COIP) es un importante paso en la evolución jurídica del Ecuador hacia el fomento de la ciberseguridad y la defensa de la privacidad de los datos. Este proyecto de ley definé y clasifica el carding como un delito cibernético, lo que indica que el Estado está decidido a luchar contra tales delitos y garantizar los derechos digitales de sus ciudadanos. Por lo tanto, a través de esta reforma se pretende no sólo proteger los derechos de los usuarios sino también dejar claro que Ecuador se ha adaptado para afrontar los desafíos actuales y futuros del mundo digital.

Conclusiones

Se ha podido determinar que existe una constante vulneración a derechos constitucionales en contra de las víctimas referente al delito de Carding, del mismo modo, se identificó que es necesario fortalecer los sistemas bancarios con programas informáticos que permitan una mayor protección de datos perteneciente a los usuarios. Con ello, se pretende que se garanticen ciberespacios seguros a fin de que los usuarios consideren que sus datos personales son usados correctamente.

Se ha determinado mediante la utilización de malware informáticos y técnicas como lo son el uso del phishing, smishing, fishing, entre otros métodos que los delincuentes informáticos pueden cometer con mayor facilidad dicho delito y con ello se evidencia la carencia que existe en los sistemas bancarios. Así mismo, se ha comprobado que las entidades bancarias no gozan de herramientas de prevención y protección suficientes respecto a las contraseñas de las tarjetas de los usuarios, ya que estas fácilmente podrían ser duplicadas o suplantadas mediante el método del skimmer.

Se identificó que en otros países ya existen ciertas herramientas para combatir eficazmente este tipo de crímenes mediante la prevención y persecución de delitos cibernéticos, así como existen medidas para proteger los datos financieros y personales de los ciudadanos. Por ello, al examinar dichas prácticas internacionales, se pudo dimensionar tanto su aplicabilidad como beneficios dentro del contexto legal ecuatoriano, con ello respaldando la necesidad de reformas legales urgentes a fin de fortalecer la protección contra la apropiación fraudulenta por medios electrónicos y el delito de carding.

Se pudo comprobar que es necesario introducir una reforma al marco legal ecuatoriano para abordar específicamente el delito de Carding, una modalidad de fraude cibernético cada vez más frecuente y perjudicial, que pone en riesgo la seguridad jurídica de los usuarios afectados por estos delitos, proporcionando un marco legal claro y específico que permita la prevención, persecución y sanción efectiva de este tipo de actividades ilícitas.

Recomendaciones

Se recomienda la implementación de aplicaciones informáticas de alto nivel en el sistema bancario ecuatoriano, mismos que posteriormente puedan considerarse como un medio para brindar seguridad a los datos de los usuarios, protegiendo de esta forma los derechos constitucionales. Esto incluye el pago de grandes cantidades de dinero, por la compra e instalación de tecnologías de seguridad innovadoras, que a su vez van seguidas de un estricto establecimiento de todas las posibles medidas de detección y prevención de actividades fraudulentas, como el Carding.

Se sugiere a las entidades bancarias en Ecuador, la inversión en tecnología de ciberseguridad, ya que esto ayudará a prevenir la pérdida de contraseñas y el fraude de los usuarios. Esto se puede lograr mediante métodos como códigos OTP o biometría, capacitar al personal para detectar ciberataques e implementar medidas proactivas contra el phishing y demás delitos cibernéticos.

Del mismo modo, se sugiere la implementación de prácticas internacionales, mismas que deben investigarse e incorporarse a la prevención y el enjuiciamiento exitosos de los delitos de Carding junto con otros delitos cibernéticos dentro de la legislación ecuatoriana. Esto incluye el uso de medidas de protección contra violaciones de datos personales y financieros, así como la asociación con agencias internacionales que se ocupan de la lucha contra el cibercrimen.

Se recomienda a los legisladores introducir una reforma específica para el delito de Carding, así como otros fraudes cibernéticos. Esta reforma debería implementar un mecanismo legal que sea fácil de aplicar respecto al cometimiento de acciones maliciosas que violan los derechos de los usuarios. Además, se recomienda que esta reforma tome como base las mejores prácticas internacionales, en concordancia con lo manifestado por expertos locales en ciberseguridad y protección de datos que puedan ayudar a adaptar su eficacia y adecuación a las particularidades del contexto ecuatoriano.

Referencias

Gómez, J. (diciembre de 2022). *IDENTIFICACIÓN DEL SUJETO ACTIVO EN EL DELITO DE ESTAFA A TRAVÉS DE MEDIOS DIGITALES Y ELECTRÓNICOS BAJO LA PERSPECTIVA DEL COIP EN EL ECUADOR''.* Universidad Internacional del Ecuador, Quito. https://repositorio.uide.edu.ec/bitstream/37000/5790/1/UIDE-Q-TDR-2023-5.pdf. Obtenido de UNIVERSIDAD INTERNACIONAL DEL ECUADOR: [Tesis de grado, Universidad Internacional del Ecuador] https://repositorio.uide.edu.ec/bitstream/37000/5790/1/UIDE-Q-TDR-2023-5.pdf

Sain, G. (2015). *Evolución histórica de los delitos informáticos*. Obtenido de Revista pensamiento penal: https://www.pensamientopenal.com.ar/system/files/2015/04/doctrina40877.pdf

Yari, J. (2023). *Análisis del proceso de identificación del sujeto activo en el delito de Apropiación Fraudulenta por Medios Electrónicos en el Ecuador en el año 2021.* [Tesis de grado, Universidad Ecotec] https://repositorio.ecotec.edu.ec/bitstream/123456789/840/1/YARI%20BUSTAMANTE%20JOSE%20ANDRE.pdf.

Acurio, S. (2012). *Delitos Informáticos: Generalidades.*

Huerta, M., & Líbano, C. (1996). Delitos informáticos. *Ed. Jurídica ConoSur.*, 17.

Torres, M. (2022). *DELITO DE APROPIACIÓN FRAUDULENTA POR MEDIOS ELECTRÓNICOS BAJO LA MODALIDAD DE PHISING DENTRO DEL MARCO JURÍDICO ECUATORIANO*. Obtenido de Universidad del Azuay: [Tesis de grado, Universidad del Azuay] https://dspace.uazuay.edu.ec/bitstream/datos/12380/1/17907.pdf

Hernández, L. A. (2023). *Delitos informáticos en Ecuador: Análisis de la intervención penal en casos de estafas mediante redes sociales.* Obtenido de Revista Científica Multidisciplinar G-Nerando.

Belcic, I. (19 de enero de 2023). *¿Qué es el malware y cómo protegerse de los ataques?* Obtenido de Avast: https://www.avast.com/es-es/c-malware

Patiño Corona, J. (09 de 08 de 2009). *Pharming, la Evolución de un Ataque*. Obtenido de Red de Repositorios Latinoamericanos: https://repositorioslatinoamericanos.uchile.cl/handle/2250/4192670

García, A. (2020). *ESTUDIO SOBRE LA INGENIERÍA SOCIAL Y SU IMPACTO EN LAS ENTIDADES ESTATALES*. Obtenido de MARVER ALBERTO BASTO GARCÍA: https://repository.unad.edu.co/jspui/bitstream/10596/34150/1/mabastoga.pdf

Yari, J. (2023). *Análisis del proceso de identificación del sujeto activo en el delito de Apropiación Fraudulenta por Medios Electrónicos en el Ecuador en el año 2021.* Obtenido de [Tesis de grado, Universidad Ecotec] file:///C:/Users/lenovo/Downloads/YARI%20BUSTAMANTE%20JOSE%20ANDRE-TESIS.pdf

Constitución de la República del Ecuador. (2008). *Constitución de la República del Ecuador.* Obtenido de https://www.gob.ec/sites/default/files/regulations/2020-06/CONSTITUCION%202008.pdf

Resolución No. JB-2010-1782. (2010). *Resolución No. JB-2010-1782 de 2010. (SUPERBANCOS)*. Obtenido de superbancos: https://www.superbancos.gob.ec/bancos/codigo-de-derechos-del-usuario-financiero/

Campos, L. M. (30 de enero de 2014). *DERECHOS DE LAS VÍCTIMAS EN EL PROCESO PENAL*. Obtenido de Derecho Ecuador: https://derechoecuador.com/derechos-de-las-victimas-en-el-proceso-penal/

Argudo, O. (2018). *Medidas cautelares y medidas de protección*. Obtenido de UNEMI: https://sga.unemi.edu.ec/media/archivologo/2022/03/04/archivologocompendio_20223492830.pdf

Código Orgánico Integral Penal. (2014). *Código Orgánico Integral Penal*. Obtenido de https://irp.cdn-website.com/e8ea09e2/files/uploaded/COIP%202023.pdf

Código Penal de la Nación Argentina. (1984). *Código Penal de la Nación Argentina.* Obtenido de https://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/16546/texact.htm

El Tiempo. (25 de diciembre de 2022). El Carding o los delitos cometidos a través del uso de tarjetas de crédito. *El Tiempo*(https://www.diarioeltiempo.com.ar/nota-el-carding-o-los-delitos-cometidos-a-traves-del-uso-de-tarjetas-de-credito-190418), pág. 1.

Tráves, N. (2018). *La vulneración de los Derechos Constitucionales por la falta de tipificación de las nuevas conductas delictivas a través de las Tecnologías de Informática y Comunicación (TICs) [Tesis de grado para la obtención del título de Abogado, UCE] .*

Arias, R., & Manzano, L. (1 de abril de 2023). EL TERRORISMO Y SU TRANSFORMACIÓN. *1*(https://dx.doi.org/10.24133/RCSD.VOL16.N01.2023.10), 142.

Código Penal Federal . (2018). *Código Penal Federal .* Obtenido de https://www.gob.mx/cms/uploads/attachment/file/422557/CODIGO_PENAL_FEDERAL.pdf

Aboitiz, F. (26 de junio de 2023). INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE ADICIONA UNA FRACCIÓN XXII AL ARTÍCULO 387 DEL CÓDIGO PENAL FEDERAL. *1*(https://www.congresocdmx.gob.mx/media/documentos/5aded1cf1f8e854711e467a6cd3e64fb09637b20.pdf), 5.

Código Penal Colombiano. (2009). *Código Penal Colombiano*. Obtenido de https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Caldas, M. (29 de agosto de 2020). *Desarticulado grupo delincuencial "Carding", dedicados al hurto por medios informáticos en la ciudad de Manizales*. Obtenido de POLICÍA NACIONAL DE COLOMBIA: https://www.bing.com/search?pglt=43&q=delito+del+carding+en+la+Legislaci%C3%B3n+COLOMBIANA&cvid=1483c3f3a5f34190894a518fded836bc&gs_lcrp=EgZjaHJvbWUyBggAEEUYOdIBBzk1MmowajGoAgCwAgA&FORM=ANNTA1&PC=LCTS

Acosta, C. (2021). *¿Qué castigos estipula el Código Penal para los delitos informáticos como la estafa?*

Anexos

Entrevistas a Profesionales del Derecho respecto al Delito de Apropiación Fraudulenta por Medios Electrónicos en el Sistema Bancario y sus Implicaciones Jurídicas en la Violación de Derechos Constitucionales

Objetivo: Obtener información sobre el delito de apropiación fraudulenta por medios electrónicos en el sistema bancario, mediante la realización de un cuestionario de preguntas a profesionales del derecho, para comprender los efectos jurídicos relacionados con la violación de derechos constitucionales.

Entrevista número 1

Entrevistado: nombre

Título académico:

Cargos desempeñados:

Cuestionario de Preguntas:

1. Desde su experiencia profesional, ¿cuáles son los desafíos más significativos que enfrentan los fiscales en la investigación y acusación de casos relacionados con la apropiación fraudulenta por medios electrónicos en el ámbito del sistema bancario?
2. ¿Cuáles serían los derechos constitucionales vulnerados derivados de los casos de apropiación fraudulenta por medios electrónicos?
3. Según su opinión ¿Cuáles serían las medidas legales más efectivas para abordar y prevenir el delito de apropiación fraudulenta por medios electrónicos en el ámbito bancario?
4. ¿Cuál es su punto de vista respecto al rápido avance tecnológico que ha influido en la interpretación y aplicación de las leyes sobre apropiación fraudulenta por medios electrónicos?
5. ¿Cómo evalúa la complejidad legal al abordar y tipificar el delito de carding en Ecuador, específicamente en relación con la seguridad jurídica del usuario?
6. ¿Cuáles son las implicaciones específicas de la adición del delito de carding en la reforma del COIP en relación con la apropiación fraudulenta por medios electrónicos a través del sistema bancario?