PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE IBARRA

ESCUELA DE JURISPRUDENCIA

TRABAJO FINAL DE TITULACIÓN

TEMA:

ESTUDIO JURÍDICO DEL ARTÍCULO 190 DEL CÓDIGO ORGÁNICO INTEGRAL PENAL SOBRE LAAPROPIACIÓN FRAUDULENTA POR MEDIOS ELECTRÓNICOS EN LA PROVINCIA DE IMBABURA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE

ABOGADO

LÍNEA DE INVESTIGACIÓN:

Derecho, participación, gobernanza, regímenes políticos e institucionalidad

AUTOR: Guamán Terán Carlos Eduardo

ASESOR: Ph.D. Bartolomé Gil Osuna

IBARRA, MAYO 2023

Ibarra, 22 de mayo de 2023

Ph.D. Bartolomé Gil Osuna

ASESOR

CERTIFICA:

Haber revisado el presente informe final de investigación, que se ajusta a las normas vigentes en la Escuela de Jurisprudencia de la Pontificia Universidad Católica del Ecuador Sede Ibarra (PUCE-SI), por lo que autorizo su presentación para los fines legales pertinentes.

…….

Ph.D. Bartolomé Gil Osuna

C.C.: 1758922585

PÁGINA DE APROBACIÓN DEL TRIBUNAL

El jurado examinador, aprueba el presente informe de investigación en nombre de la Pontificia Universidad Católica del Ecuador Sede Ibarra PUCE-SI:

(f)……

PhD. Bartolomé Gil Osuna

C.C.: 1758922585

(f)……

Mgs. María Rosario Espinoza Andrade

C.C.: 1003155130

(f)……

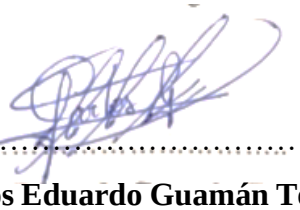
PhD. Marilena Asprino Salas

C.C.: 1758069494

ACTA DE CESIÓN DE DERECHOS

Yo, **Carlos Eduardo Guamán Terán**, declaro conocer y aceptar la disposición del Art. 165 del Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación que manifiesta textualmente: "Se reconoce facultad de los autores y demás titulares de derechos de disponer de sus derechos o autorizar las utilizaciones de sus obras o prestaciones, a título gratuito u oneroso, según las condiciones que determinen. Esta facultad podrá ejercerse mediante licencias libres, abiertas y otros modelos alternativos de licenciamiento o la renuncia"

Ibarra, 22 de mayo de 2023.



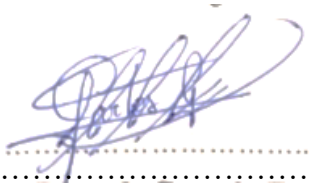
(f)……

Carlos Eduardo Guamán Terán

C.C. 1003798798

AUTORÍA

Yo, **Carlos Eduardo Guamán Terán**, portador de la cédula de ciudadanía N° 1003798798, declaro que la presente investigación es de total responsabilidad del autor, y eximo expresamente a la Pontificia Universidad Católica del Ecuador Sede Ibarra de posibles reclamos o acciones legales.



(f)…….

Carlos Eduardo Guamán Terán

C.C. 1003798798

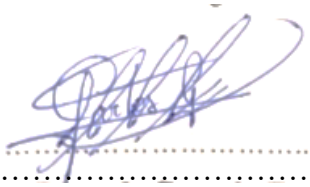
DECLARACIÓN y AUTORIZACIÓN

Yo, **Carlos Eduardo Guamán Terán**, portador de la cédula de ciudadanía N° 1003798798, autor del trabajo de grado titulado: "Estudio jurídico del Artículo 190 del Código Orgánico Integral Penal sobre la apropiación fraudulenta por medios electrónicos en la Provincia de Imbabura", previo a la obtención del título profesional de "Abogado", en la Escuela de Jurisprudencia.

1.- Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador Sede-Ibarra, de conformidad con el artículo 144 de la Ley Orgánicade Educación Superior de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la Pontificia Universidad Católica del Ecuador Sede Ibarra a difundir a través del Repositorio Digital de la PUCESI el referido trabajo de graduación, respetando las políticas de propiedad intelectual de la Universidad.

Ibarra, 22 de mayo de 2023.



(f)……

Carlos Eduardo Guamán TeránC.C. 1003798798

AGRADECIMIENTO

A Dios por su infinito amor quien nos da la vida y nos guía por el sendero correcto para encaminarme en el bien y la verdad.

A la Facultad de Jurisprudencia de la Pontificia Universidad Católica del Ecuador Sede Ibarra PUCE-SI, por permitirme avanzar día a día en el conocimiento de la Ciencia de Derecho, tengo que expresar el reconocimiento especial y mi más noble agradecimiento a mis distinguidos catedráticos, quienes han sabido enrumbarme por el camino del saber para formarme y convertirme en el futuro profesional del derecho, capaz de aplicar lo teórico y lo práctico, apegado a los valores éticos, morales, y los servicios a la colectividad.

Un agradecimiento muy especial a mí asesor Dr. Bartolomé Gil Osuna, por su constante y acertado asesoramiento, apoyo y comprensión.

Carlos Eduardo Guamán Terán

DEDICATORIA

A Dios, por darme la oportunidad de vivir y por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente y por haber puesto en mi camino a aquellas personas que han sido mi soporte y compañía durante todo mi periodo de estudio.

A mis padres, mis hermanas por darme la vida, por ser el pilar fundamental en todo lo que soy, en toda mi educación, tanto académica, como de la vida, por su incondicional apoyo, comprensión, amor, ayuda en los momentos difíciles, y por ayudarme con los recursos necesarios para mis estudios.

A mis amigos y compañeros por apoyarme y compartir conmigo cada escalón de esta meta.

A mis maestros por su tiempo y sabiduría que me transmitieron en el desarrollo de mi formación profesional.

A todos ellos mi eterna gratitud.

Carlos Eduardo Guamán Terán.

ÍNDICE

1. RESUMEN

Las telecomunicaciones constituyen uno de los sectores de más grande desarrollo tecnológico en la sociedad, lo cual ha significado cambios en la forma de trabajar, en los estilos de vida, y en la visión general de muchos aspectos involucrados en el desarrollo económico y social de los Estados, lo que ha permitido el germen de una serie de conductas ilícitas llamadas, de forma genérica, delitos informáticos, digitales y de telecomunicaciones. Frente a esta realidad se inició esta investigación que tuvo como objetivo general el analizar desde la perspectiva tecno-jurídica la apropiación fraudulenta por medios electrónicos en la provincia de Imbabura, a fin de determinar la vulneración de los derechos de las personas. La cual tuvo como enfoque el cualitativo, con un nivel de profundidad descriptivo-explicativo, que partió de la aplicación de los métodos deductivo-inductivo, analítico sintético y exegético, que coadyuvaron en el análisis de los diferentes textos jurídicos, desde las convenciones, tratados e instrumentos internacionales debidamente ratificados hasta las normas jurídicas del ordenamiento interno ecuatoriano potencialmente aplicables al delito de apropiación fraudulenta por medios electrónicos. La técnica utilizada en este trabajo investigativo fue la revisión documental acompañada de la entrevista. Se determinó que en la actualidad el Estado ecuatoriano reconoce y brinda protección de identidad y datos a cada individuo, a finde evitar la vulneración de derechos humanos, por lo que estructura toda una normativa preventiva. No obstante, se evidenció que, en la Provincia de Imbabura, los datos sobre apropiación indebida por medios electrónicos son escasos, presumiéndose que son frecuentes estas conductas delictuales, pero los usuarios víctimas de estos delitos de cuello blanco no denuncian frente a las autoridades competentes.

Palabras clave: Apropiación fraudulenta por medios electrónicos, seguridad jurídica, delitos informáticos, crimen cibernético, medios electrónicos.

2. ABSTRACT

Telecommunications constitute one of the sectors with the greatest technological development in society, which has meant changes in the way of working, in lifestyles, and in the general vision of many aspects involved in the economic and social development of the countries. States, which has allowed the germ of a series of illicit conducts called, generically, computer, digital and telecommunications crimes. Faced with this reality, this investigation began with the general objective of analyzing fraudulent appropriation by electronic means in the Province of Imbabura from a techno-legal perspective, in order to determine the violation of people's rights. Which had a qualitative approach, with a descriptive-explanatory level of depth, which started from the application of deductive-inductive, synthetic analytical and exegetical methods, which contributed to the analysis of different legal texts, from conventions, treaties and duly ratified international instruments up to the legal norms of the Ecuadorian internal legal system potentially applicable to the crime of fraudulent appropriation by electronic means. The technique used in this investigative work was the documentary review accompanied by the interview. It was determined that currently the Ecuadorian State recognizes and provides identity and data protection to each individual, in order to avoid the violation of human rights, for which reason it structures an entire preventive regulation. However, it was evidenced that, in the Province of Imbabura, the data on misappropriation by electronic means is scarce, presuming that these criminal behaviors are frequent, but the users who are victims of these white-collar crimes do not report them to the competent authorities.

Keywords: Fraudulent appropriation by electronic means, legal security, computer crimes, cybercrime, electronic means

3. INTRODUCCIÓN

En la última década el delito de apropiación fraudulenta por medios electrónicos ha tomado trascendencia jurídica, debido al surgimiento y rápido desarrollo de este delito, implicando un nivel de riesgo financiero significativo que puede afectar negativamente los márgenes de utilidad y ganancia de las personas tanto naturales como jurídicas y la imagen de una entidad económica, provocado por un hecho punible que, sin duda, plantea la necesidad de avanzar hacia una sociedad digital sostenible en el marco del impacto sistémico de la disrupción digital que ha proliferado conductas delictuosas.

Los delitos informáticos, llamados también delitos cibernéticos, delitos electrónicos, delitos relacionados con las computadoras, delincuencia relacionada con el ordenador, o crímenes informáticos, han llegado a niveles organizacionales, por lo que se indispensable definirlos, como lo hacen Acosta, Benavides y García (2020), quienes consideran que “son actos ilícitos cometidos mediante el uso inadecuado de la tecnología, atentando contra la privacidad de la información de terceras personas, dañando o extrayendo cualquier tipo de datos que se encuentren almacenados en servidores o *gadgets*” (p. 2), en concordancia con lo expresado por la Organización para la Cooperación Económica y el Desarrollo (2021), como: "Cualquier conducta ilegal, no ética o no autorizada que involucra el procesamiento automatizado de datos y/o la transmisión de datos" (p. 3).

En tal sentido, la seguridad informática se erige como un derecho elemental dentro de la sociedad, por lo que es indispensable determinar los diferentes tipos de delitos informáticos existentes, entre los que resalta, la apropiación fraudulenta por medios electrónicos, para contar con herramientas de vanguardia que contribuyan a enfrentar y encarar, de manera efectiva, las derivaciones tanto personales, como económicas y sociales de estos actos delictivos en los que es indefectible velar por los derechos de las víctimas.

Todo ello, hace indispensable también tener un conocimiento preciso sobre los riesgos que significa, el hecho voluntario de confiar, de manera directa, información de primer nivel ─personal, empresarial o financiera─ a aplicaciones, sitios o *web side*, que son

susceptibles de ser vulnerados por personas ─profesionales de oficio─ como son los *hackers*, *crackers*, *phrackers* o piratas informáticos que convierten a los usuarios o cibernautas en víctimas de fraude, chantaje o extorsión tomando en cuenta los medios electrónicos.

Esto evidencia deficiencias en los sistemas de detección del crimen electrónico; lo que conduce a que estos delitos deben ser investigados de manera exhaustiva por parte de los organismos de seguridad del Estado, como aseguran Naranjo, Mendoza, Alonso e Hinojosa (2020):

> El empleo de las nuevas tecnologías de la información y las comunicaciones en la consumación del delito, que ha significado la ruptura del uso de los convencionales *modus operandi*, trajo aparejado el surgimiento y consolidación de una nueva especialidad de la técnica y la informática criminalística. (p. 256)

Esta nueva especialidad es la informática criminalística que impone nuevos retos, en el país, para coadyuvar en el esclarecimiento completo, objetivo y multilateral de este tipo de delitos, que se presentan como complejos, debido a la diversidad de factores que inciden en la comisión de estos. Frente a esta realidad, los Estados y las organizaciones nacionales e internacionales parecen incapaces de responder, con la misma rapidez o eficacia, al peligro del desarrollo de nuevos delitos informáticos.

Como bien señala la Organización de Naciones Unidad, en la CEPAL (2022)

> Desde fines de los años ochenta, la revolución digital ha transformado la economía y la sociedad. Primeramente, se desarrolló una economía conectada, caracterizada por la masificación del uso de Internet y por el despliegue de redes de banda ancha. Luego, se desarrolló una economía digital resultado de la expansión del uso de plataformas digitales como modelos de negocios de oferta de bienes y servicios. Y ahora se avanza hacia una economía digitalizada que basa sus modelos de producción y consumo en la incorporación de tecnologías digitales en todas las dimensiones económicas, sociales y medioambientales. (p. 11)

Esta realidad que involucra a todos, es el resultado de la adopción y de la integración de tecnologías digitales muy avanzadas (redes móviles de quinta generación (5G), internet

de las cosas (IoT), computación en la nube, inteligencia artificial, analítica de grandes datos, robótica, entre otras) que contribuyen a que se esté pasando de un mundo híper conectado a un mundo digitalizado en las dimensiones económicas y sociales, que la convierten en un escenario propio para la comisión de delitos en "estos ecosistemas complejos que se encuentran en proceso de adecuación organizativa, institucional y normativa" (CEPAL, 2022, p. 24).

El rol del Estado Constitucional de derechos y justicia es garantizar una adecuada protección de datos de cada individuo frente a la necesidad de ajustar las normas con el propósito de crear un ámbito de igualdad de condiciones para los operadores económicos quienes deben gozar de seguridad jurídica; pero lastimosamente, el progreso de la técnica en general y de la informática, en particular, como asevera Herrera (2018) "no han sido acompañadas de defensas adecuadas que permitan hacer frente a la mala utilización de las mismas" (p. 12).

Este ha hecho que, la apropiación fraudulenta por medios electrónicos, en medio de esta gama de delitos informáticos, haya sido tipificada en el marco normativo específico para lograr la protección del derecho fundamental a la protección de datos personales en el Código Orgánico Integral Penal (en adelante COIP) 2014, relacionada con la regulación del tratamiento de la información personal tanto en las disposiciones de la Ley del Sistema Nacional de Registro de Datos Públicos, Ley Orgánica de Comunicación y Ley Orgánica de Telecomunicaciones.

El propósito que motivó la realización de la presente investigación fue el creciente interés del tema en el contexto del derecho digital o informático, ya que forma parte de las nuevas realidades del Ecuador, y un aspecto en particular que se pudo evidenciar, fue que la mayoría de estos delitos cometidos a través de medios electrónicos quedan en la oscura impunidad, debido, entre otras cosas, a su dificultad en determinar su antijuricidad o la falta de denuncia, aunado a la falta de preparación de las autoridades encargadas de la persecución de los mismos, así como la carencia de un presupuesto razonable para investigar e indagar el procedimiento adecuado frente a la proliferación de estos delitos y, determinar las responsabilidades para la protección del derecho a la autodeterminación informativa.

Por lo que se formuló la siguiente interrogante, derivada de la vulnerabilidad de los sistemas informáticos o redes electrónicas y de las telecomunicaciones: ¿el incremento de los medios electrónicos y las redes sociales incide en la comisión de delitos informáticos como la apropiación fraudulenta por medios electrónicos?

Lo que condujo a establecer como objetivo general de esta investigación el analizar desde la perspectiva tecno-jurídica la apropiación fraudulenta por medios electrónicos en la Provincia de Imbabura, a fin de determinar la vulneración de los derechos de las personas. Y como objetivos específicos: a) Describir el régimen jurídico nacional e internacional que tipifica y sanciona la apropiación fraudulenta por medios electrónicos; b) Determinar cuáles son las consecuencias de la vulneración de los derechos de las personas para que estas puedan prevenirse y c) Exponer las características esenciales de la apropiación fraudulenta por medios electrónicos en la Provincia de Imbabura con el fin de conocer y erradicar en la práctica este tipo penal digital, debido a la carencia de parámetros jurídicos y doctrinales respecto al mismo.

El incremento desmesurado de la tecnología y de nuevas redes sociales en el país trae consigo también el aumento y el agravio de los delitos informáticos como la apropiación fraudulenta por medios electrónicos, objeto de estudio de esta investigación, como la estafa a través de medios electrónicos, la revelación ilegal de base de datos, transferencia electrónica de activo patrimonial, ataque a la integridad de sistemas informáticos o la reprogramación o modificación de información de equipos terminales móviles, entre otros, que permite vincular este estudio con la línea de investigación N° 13 de la PUCE 2017 Derecho, participación, gobernanza, regímenes políticos e institucionalidad y con el Plan Nacional Generando Oportunidades 2021-2025, diseñado por el Estado, alineado con el Plan de Gobierno 2021-2025 y la Agenda 2030 de Desarrollo Sostenible, estructurado en 5 ejes y 16 objetivos, según el cual, en su eje institucional y objetivo 14 prevalece el fortalecimiento de las capacidades del Estado con énfasis en la administración de justicia y eficiencia en los procesos de regulación y control, con independencia y autonomía, que plantea objetivos y políticas para el reconocimiento igualitario de los derechos de todos los individuos. De esta manera, el sistema judicial es un pilar para la defensa de las libertades y las garantías de los derechos de todos los ecuatorianos.

A sabiendas que las tecnologías digitales han crecido exponencialmente y su práctica se ha globalizado, gracias a la masificación del uso de teléfonos inteligentes y al consiguiente acceso a la información y a la aparición de novedosas redes sociales, que hacen vulnerables los sistemas tecnológicos, hicieron que la investigación estuviera dirigida a profesionales del derecho, los cuales compartirán su punto de vista frente al tema de la apropiación fraudulenta por medios electrónicos, frente a sus consecuencias lesivas al patrimonio de las personas, se convierten en los principales beneficiarios. Teniendo en cuenta que dichos profesionales pueden tomar en cuenta el presente estudio para aplicarlo y llevarlo a la práctica en el libre ejercicio y orientar a los particulares sobre la situación de vulnerabilidad del uso de los medios tecnológicos, pues, estos dan pie al cometimiento de delitos informáticos.

4. ESTADO DEL ARTE

Los avances en la tipicidad del delito de apropiación fraudulenta por medios electrónicos transforman el fraude contra los individuos, que ahora trasciende en el Estado ecuatoriano, ya que se evalúa, con más precisión, la seguridad de la información de organizaciones, entidades bancarias y de los ciudadanos, que incluye confidencialidad, integridad y disponibilidad, es decir, que cualquier actividad comercial que utilice prácticas o dispositivos engañosos para privar a otra persona de la propiedad u otros derechos es debidamente regulada por las disposiciones penales.

Por lo que en este apartado se inició con la finalidad de determinar en qué estado de conocimiento se encuentra el delito de apropiación fraudulenta por medios electrónicos; lo que conllevó a la revisión bibliográfico documental a través de la búsqueda y selección de trabajos científicos de varios autores, que conforman la doctrina nacional e internacional, sobre esta institución jurídico penal, en repositorios digitales de google académico, en bases de datos de revistas indexadas, en tratados internacionales y en la legislación ecuatoriana, para fortalecer y contribuir en el análisis de los delitos informáticos que aquejan a la sociedad internauta.

Por medio de investigaciones como ésta, aseguran Acosta, Benavides y García (2020), en su publicación intitulada Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios,

> Se determinan los tipos de delitos informáticos, para conocer las debilidades de las organizaciones en este sentido y accionar una serie de controles necesarios para resguardar la información cibernética e ir combatiendo mediante claves, encriptaciones y niveles de seguridad todo lo concerniente al plagio de información. También se analiza la impunidad, desde el punto de vista legal y, sus consecuencias hacia terceras personas (implicados), que se ven involucrados en el hecho delictivo. (p. 2)

Estas circunstancias, se dan en un contexto, en que el uso de la informática, a nivel global, mantiene un repunte importante convirtiéndose en un escenario indispensable

para la sociedad. El solo hecho de brindar servicios a los usuarios que les permite simplificar sus actuaciones, sobre todo para informarse, comunicarse y poder interactuar,lo convierte en una herramienta indefectible y, en muchos casos, útil y necesaria.

> La modernización ha traído consigo, aseveran estos autores, "que el manejo de la información, se realice mediante procesadores informáticos, que permiten almacenar una cantidad considerable de información y, que, al mismo tiempo, se pueda acceder de manera rápida a esos datos. La información puede ser de cualquiertipo (personal, empresarial, financiera-bancaria, societaria), siendo esta apetecida por los llamados delincuentes informáticos con la intención de sacar provecho de tipo oneroso, por medios de chantajes, desprestigio y hasta secuestro de la información sustraída. (p. 5)

Este conjunto de comportamientos que generan delitos tipificados en la normapenal, debe ser normado, con gran sutileza, debido a que traen como consecuencia severos daños a terceras personas, ocasionándoles diferentes lesiones y, en diversos casos, van acompañados de pérdidas de bienes jurídicos protegidos, fundándose en la divulgación y transmisión de datos en la red que no son autorizados, yendo en contra de la ética.

Debido a ello, la Fiscalía General del Estado (2021) publicó un trabajo, bastante interesante, intitulado Ciberdelitos, en el que pretende, entre otros temas, el habilitar un ciberespacio más seguro, que incluye:

- Crear un entorno digital más limpio y saludable.
- Tomar desde el Gobierno la iniciativa para asegurar la infraestructura digital que impulsa la economía digital y que respalde el desarrollo de un entorno digital saludable.
- Motivar a que empresas, organizaciones y personas sean también los responsables de asegurar su entorno digital.
- Mejorar la cooperación internacional, que comprende: • Fomentar un ciberespacio abierto, seguro, estable, accesible, pacífico e interoperable. • Promover el desarrollo y la implementación de normas voluntarias y no vinculantes, alineadas al derecho internacional. • Desarrollo y adopción de

estándares técnicos e interoperables. • Intensificar la cooperación con socios internacionales para combatir las ciber amenazas transfronterizas.

- Y por último, el Gobierno incluye en sus estrategias alentar a personas interesadas en la ciberseguridad a que mejoren sus habilidades a través de la participación en programas de recompensas "*bug bounty*", ejercicios cibernéticos nacionales, institucionalidad de ciberseguridad, programasacadémicos especializados, leyes específicas, acuerdos internacionales,incentivos para fomentar la investigación y creación de soluciones, pueden ser, entre otras actividades, las necesarias para fortalecer la ciberseguridad en el Ecuador. (p. 51)

La Fiscalía General del Estado es consciente que la dependencia de la sociedad a las nuevas tecnologías de la información y de las comunicaciones (TIC) evidencia el daño latente que ocasiona en la sociedad la delincuencia informática. El creciente número de personas dedicadas a cometer este tipo de delitos a través de medios electrónicos hace inminente el estudio de las implicaciones sociales de este nuevo flagelo delictual, que conlleve a la necesidad de regular las nuevas tendencias delictuales, analizando estos nuevos escenarios desde donde actúan y llevan a cabo el deterioro del patrimonio tanto de personas naturales como jurídicas.

Este escenario delincuencial hace vulnerable a la seguridad como bien público; por lo que no solo la seguridad en el mundo *offline*, sino también la seguridad en el ciberespacio –*online*– es concebido un valor elemental que el Estado debe garantizar. Por lo que, en Ecuador, conscientes de la necesidad de implementar una normativa que contribuya al combate efectivo de la criminalidad informática, se ha incluido dentro de la Constitución de la República del Ecuador la responsabilidad estatal de desarrollar y llevar a cabo políticas públicas direccionadas a proteger los derechos de las personas, en particular, brindar protección al uso adecuado del ciberespacio.

No es sencillo combatir el ciberdelito, de manera efectiva, pero si se proponen mecanismos para reconocer e identificar su inicio, sus motivaciones, sus causas y múltiples actores, podremos encontrar herramientas de combate eficientes que contribuirían a

minimizar sus efectos y consecuencias. Como señala La Fiscalía General del Estado (2021) "Todo ello transcribe políticas nacionales, empresariales y personales, así como la creación de métodos y herramientas tecnológicas que permitan al usuario ejercer pragmáticamente el derecho a protegerse. En este escenario, además, la idoneidad del derecho penal es de gran importancia para el enjuiciamiento del delito cibernético, ya sea nacional o internacional" (p. 10).

En la legislación ecuatoriana, al hacer referencia al delito informático de apropiación fraudulenta por medios electrónicos, señala Sempertegui (2022), en su trabajo denominado Delitos de apropiación fraudulenta por medios electrónicos bajo la modalidad de *phishing* dentro del marco jurídico ecuatoriano, destaca que "el bien jurídico protegido es la propiedad; no obstante, en otros países de la región, este delito se encuentra en el apartado de delitos económicos" (p. 32). Esto se debe, entre otras cosas, a que la comisión de este delito trae consecuencias negativas desde un punto de vista individual y también colectivo, llegando a ocasionar lesiones a agentes comerciales, y cuando es un delito de alta escala puede afectar, incluso el orden económico de un Estado.

En este tipo de delitos, el engaño es el epicentro de la actuación delictiva, que generalmente se lleva a cabo a través de correos electrónicos, los que, con frecuencia, tienen enlaces a un sitio *web* falso, con apariencia de ser un *web side* legítimo. Los usuarios, que no se percatan de nada, una vez están en el sitio falso, son vilmente engañados con el propósito de ingresar con sus datos confidenciales, lo cual trae como consecuencia que los delincuentes, ahora, cuenten con un amplio margen de actuación que les permite cometer estafas y fraudes con todos los datos confidenciales que han obtenido.

El *modus operandi* de los delincuentes es cada día más sofisticado, como afirma Sempertegui (2022),

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

> humanos o tecnología o de áreas comerciales relacionadas a transacciones financieras. (p. 36)

Sin olvidar que otra modalidad, puede ser la realizada por fax, por mensajes de *whatsApp*, por *facebook*, en los cuales se publican premios y descuentos muy atractivos en la venta de algunos productos, de consumo masivo. Estos mensajes tienen como destinatario final genérico, no se envía a alguien en particular; por lo cual el contenido de estos mensajes, muy bien diseñados, son enviados de forma masiva para lograr, de manera inmediata, una gran cantidad de usuarios, quienes saben muy bien que un porcentaje de usuarios incautos —por mínimo que sea— caerán en la jugada e ingresarán al sitio falso, donde serán presa fácil para extraer información confidencial muy valiosa para cometer, posteriormente sus delitos.

En este contexto, la administración de justicia se hace ineficiente, como asegura Acurio (2019),

> se ha podido evidenciar el incremento de la impunidad, por la falta de normativa, y medios adecuados para la investigación y juzgamiento de estos delitos, pues, se debe entender desde la función legislativa, que no es posible aplicar los mismos preceptos legales para aquellas conductas que bien pueden materializarse en espacios físicos en el territorio. (p. 21)

Como se ha reiterado, los delitos informáticos se van manifestando como una modalidad delictiva creciente, derivada del mal uso de las nuevas tecnologías, lo que deriva en existencia palpable de vacíos jurídicos, no previstos por la normativa penal, que brinden adecuada protección a los bienes jurídicos susceptibles de ser objeto de ataque por parte de estos nuevos delincuentes que, en gran medida, viven en el anonimato.

Del mismo modo, se pronuncia Chitalogro (2022) en su investigación Análisis dogmático penal de los delitos de apropiación fraudulenta y estafa cuando son realizados por medios electrónicos en el COIP, quien dice que

> Esto no es una realidad única de nuestro país, sino que, en todas las legislaciones del mundo, a lo largo del tiempo, se han creado normativas incluyendo este tipo de

> delitos, dado que la inseguridad del internet, trae consigo diversos riesgos, vulnerabilidad y amenazas no solo hacia el sistema informático, sino que va más allá poniendo en riesgo derechos de las personas como son la violación a la intimidad, patrimonio, datos personales, integridad sexual y otros. (p. 16)

Esta realidad genera, a simple vista, gran preocupación debido a que el *quantum* de estos perjuicios se perfilan muy superior a la delincuencia tradicional, aunado a las posibilidades que se pueda aprehender al delincuente, pues está en el anonimato y su campo de acción es prácticamente invisible. Esto viene dado debido a que la informática es objeto de ataques y, además un medio muy propicio para la comisión de estos delitos, en particular la informática es un medio idóneo para la comisión de delitos de carácter patrimonial, ya que acumula gran cantidad de datos e información confidencial, que llega a manos de estos criminales digitales, que pareciera ser, nadie los detiene, porque a pesar que se encriptan muchos de los datos, por parte de los usuarios privados y públicos, logran acceso a ellos y manipularlos.

Es indudable que el desconocimiento de las nuevas modalidades ciber delictivas, al lado de la falta de capacitación adecuada y especialización de los funcionarios del cuerpo policial y funcionarios judiciales en relación a estos delitos cometidos a través de medios electrónicos hace que estas conductas delictivas no sean perseguidas con eficiencia, por lo que es inminente que se adopte una legislación avanzada en el combate del crimen cibernético, una cooperación y coordinación entre los cuerpos policiales y administradores de justicia para enfrentar, de manera más efectiva la proliferación de estos delitos.

De esta manera, el acceso directo a información valiosa de los usuarios, hace que las redes sociales sea un terreno abonado para la comisión de delitos de carácter informático, como indica Morocho (2022) en su investigación intitulada Incidencia del delito de estafa a través de redes sociales, año 2017-2020, cantón La Libertad, en el que considera que “las diversas plataformas reúnen los requisitos necesarios para la eliminación de distintas barreras legales para el uso inadecuado del internet, sin la necesidad de realizar los actos de manera presencial, que dificulta posteriormente dar con el paradero del responsable de este daño causado mediante las redes sociales” (p. 22).

Es significativo el aporte que hace Aparicio-Izurieta (2022) en su Trabajo Delitos informáticos en Ecuador según el COIP: un análisis documental, en el que sostiene que

> las telecomunicaciones conforman uno de los sectores de más grande desarrollo tecnológico en el planeta. Las novedosas tecnologías brindan grandes ventajas para las comunidades, pero también pueden ser medios para que diversas personas tengan la posibilidad de hacer diferentes tipos de fraudes, mismos que afectan a usuarios, operadores de telecomunicaciones y proveedores de servicios a nivel general, ocasionando valiosas pérdidas no solo económicas sino también humanas. (p. 1058)

Partiendo de ello, se afirma que los delitos informáticos, al igual que otro tipo de delito, van dirigidos a obtener un beneficio económico para quien los comete y causan, por vía de consecuencia, una pérdida para quien los sufre, por lo que esta relación causa efecto hace ineludible las sanciones que deben imponerse a este tipo de delitos para lograr un equilibrio en la balanza entre estos dos factores y exista, en cierta medida, una igualdad entre la víctima y el victimario.

5. MATERIALES Y MÉTODOS

La presente investigación tiene un enfoque cualitativo debido a que se realizó la recolección de información a través de la observación participativa, representada por los diferentes autores que analizan el tema desde diversas perspectivas, analizando los datos obtenidos en base a los sistemas de banca electrónica, el sistema bancario y de quienes administran justicia dentro de este delito, empleando el análisis profundo dentro de la doctrina, teoría, jurisprudencia y legislación vigente en lo referente al objeto de estudio.

En cuanto al nivel de profundidad de la investigación fue descriptivo debido a que se procedió a detallar el estado de la investigación y la problemática actual de la apropiación fraudulenta por medios electrónicos, tomando en cuenta los elementos objetivos y subjetivos del delito, así como los medios electrónicos como instrumento en el cometimiento del mencionado delito.

Este estudio investigativo partió de la aplicación de los métodos deductivo – inductivo, toda vez que, partiendo de ideas generales derivadas de la normativa vigente y opiniones doctrinarias se realizaron los aportes personales, reducidas a ideas particulares. Un método, que actualmente se ha hecho indispensable su utilización fue el analítico sintético, para lograr un estudio preciso del delito de la apropiación fraudulenta por medios electrónicos para priorizar los derechos de las víctimas de estos delitos electrónicos y el método analítico documental que permitió a la investigación realizar la revisión de datos documentales obtenidos, no solo en forma directa, sino por medio de las fuentes indirectas, información proporcionada por datos oficiales, otras investigaciones, los cuales permitieron obtener nuevos conocimientos sobre el tema que contribuyen a la erradicación de este fenómeno lesivo en el normal uso de los instrumentos electrónicos.

La aplicación del método exegético fue también indispensable para el estudio de la normativa penal y legal, porque sobre esta base se analizaron los diferentes textos jurídicos, desde las convenciones, tratados e instrumentos internacionales hasta las normas jurídicas del ordenamiento interno ecuatoriano y los diferentes instrumentos internacionales debidamente ratificados y potencialmente aplicables al delito de apropiación fraudulenta por medios electrónicos.

En relación a la técnica utilizada en este trabajo investigativo fue la revisión documental, con la cual se accedió al contenido de información explanada por diversos autores que conforman la doctrina tanto nacional como internacional que se ha venido pronunciando acerca de esta actuación delictiva. Esta revisión permitió hacer uso de repositorios digitales de google académico, bibliotecas nacionales y distintas obras: textos, ensayos, artículos científicos indexados y tesis que abordaron con anterioridad la temática. Esta fue acompañada de la entrevista como técnica que consistió en la recopilación de datos mediante el cuestionario previamente diseñado, semi-estructurado basado en preguntas abiertas sobre la apropiación fraudulenta por medios electrónicos frente a la administración de justicia, dirigida al Dr. Luis Santiago Vallejo Salazar, Dr. Alcívar Rodolfo Tulcanazo Sarabino, Dra. María Dolores Echeverría Vásquez y el Dr. Segundo Méndez Criollo, Jueces de la Unidad Judicial de Multicompetente del cantón Antonio Ante y del Juzgado Tercero de Garantías Penales, provincia de Imbabura, para recoger información especializada sobre el caso, con la finalidad de facilitar el conocimiento científico de este delito que está en creciente desarrollo en la sociedad ecuatoriana. Los instrumentos que se utilizaron fueron la ficha documental y el cuestionario.

6. RESULTADOS Y DISCUSIÓN

Dentro del derecho penal y del derecho procesal penal cuando se investiga la incidencia social de diferentes tipos penales tipificados en el COIP, sin duda una de las modalidades de delito, más frecuentes, es el delito informático o ciberdelito, el cual forma parte de la delincuencia organizada, con todas sus exposiciones tecnológicas. Como expone la Redacción Seguridad de El Diario El Comercio (2022),

> Los ataques de las ciber mafias son recurrentes en el país. Un informe estadístico de la Unidad de Ciberdelitos de la Policía muestra que desde el 2020 hasta el 6 de julio de 2022, se han registrado 3 183 delitos informáticos. En todo el 2020 fueron 682 casos; en el 2021 subieron a 1 851 y en poco más de seis meses de 2022 la Policía ya ha iniciado 650 investigaciones a escala nacional. Guayas, Pichincha, Manabí, Imbabura, Carchi y Azuay son las provincias con más casos.
>
> Cinco tipos de estos ilícitos se han cometido con mayor frecuencia en el país. Estos son: la estafa en línea, violación a la intimidad, el acceso no consentido a un sistema informático, el ataque a la integridad de sistemas informáticos y la apropiación fraudulenta por medios electrónicos.
>
> Este último es el más común. Se configura cuando una persona utiliza fraudulentamente un sistema informático o redes electrónicas para apropiarse de un bien ajeno, de transferencias de dinero o bienes no consentidos en perjuicio de una persona. Se sanciona con cárcel de uno a tres años, según el Art. 190 del COIP. (p. 1)

Esto hace inminente su estudio, desde un punto de vista científico, para determinar las causas de su proliferación y lograr que esta práctica habitual, disminuya o pueda contrarrestarse, a sabiendas que, la falta de cultura digital es característica en el país, pues, "aunque el 75.6% de la población ecuatoriana usa las nuevas tecnologías de la información como el internet, solo el 10% tiene un conocimiento digital" (Notimundo, 5 mayo 2022, párr. 2)

Por lo que los ecuatorianos, en este momento, se encuentran en una suerte de estado de indefensión digital frente a la posibilidad de la comisión de delitos informáticos. La realidad ecuatoriana evidencia ausencia de un marco legal protector de datos que se encuentran en

internet. Por lo que es conveniente que se tomen medidas para proteger la información de la nube digital. Para lo cual, Chávez (2022) como Gerente Senior de Risk Advisory de Deloitte, sugiere a los particulares y a las empresas lo siguiente:

> Realizar revisiones de seguridad periódicas, sobre todo cuando la empresa tenga aplicaciones que permitan transaccionar a los clientes y las mismas estén disponible en internet. Monitoreo de uso, almacenamiento y tránsito de información sensible continuamente. Registro y monitoreo de actividades realizadas por administradores que tienen acceso a la base de datos de la empresa.
>
> En cuanto a la protección de información personal, Chávez hace también tres recomendaciones:
>
> Evitar compartir información sensible en redes sociales (y no permitir que estas la usen públicamente). Configurar medidas de seguridad y privacidad en rede sociales y en aplicaciones móviles (por ejemplo, desactivar la geolocalización). Ser más cautelosos cuando se reciben llamadas solicitando información personal. En caso de ofertas comerciales, que suelen decir que conocen previamente nuestra información, se debe pedir que ellos den los datos y nosotros validarlos, por ejemplo, los primeros 5 dígitos de la cédula y nosotros completamos los faltantes. (p. 2)

Aunque esto no previene del todo la apropiación fraudulenta por medios electrónicos, debido a lo difícil que es hacer algo contra la actual filtración de datos, puede contribuir, en cierta medida, a prevenir este tipo de eventos delictuales, que de acuerdo con información de la Fiscalía (2020) “los más frecuentes son las estafas digitales con modalidades como suplantación de la identidad y la apropiación fraudulenta a través de medios electrónicos” (El Universo, 2020, párr. 2)

6.1. Régimen jurídico nacional e internacional de la apropiación fraudulenta por medios electrónicos

Como bien se sabe, los que cometen este tipo de delitos, generalmente poseen un vasto conocimiento en ciencias informáticas, y en algunas ocasiones, están posicionados en lugares de trabajo estratégicos, tanto en empresas e instituciones públicas como a nivel privado, lo que les permite acceder a información y datos de carácter sensible y confidenciales, lo que genera para los usuarios, en la mayoría de los casos, severos daños económicos. Por lo que el Estado ecuatoriano, consciente de que estas actuaciones delictuales no llegan a ser investigadas, o no se informa a la autoridad competente, debido a las dificultades de persecución de estos delitos, ha implementado una normativa para sancionar y combatir, de manera eficaz, la comisión de estos delitos.

En primer término, la CRE (2008) como instrumento jurídico garantista de los derechos de las personas, entabla una relación homogénea entre la sociedad, la seguridad de las personas y la información, como se puede evidenciar en la Tabla 1, con la finalidad de velar y proteger los derechos de las personas, en este sentido establece:

Tabla 1. CRE garantiza la seguridad y protección de las personas frente a delitos informáticos

Art. 3. Son deberes primordiales del Estado:	1.- Garantizar sin discriminación alguna el efectivo goce de los derechos establecidos en la Constitución. 5.- Planificar el desarrollo nacional, (…) promover el desarrollo sustentable (…), para acceder al buen vivir. 6.- Promover el desarrollo equitativo (…) 7.- Proteger el patrimonio natural y cultural del país. 8.- Garantizar a sus habitantes el derecho a una cultura de paz, a la seguridad integral.
Art. 16. Todas las personas, en forma individual o colectiva, tiene derecho a:	1.- Una comunicación libre, intercultural, incluyente, diversa y participativa, en todos los ámbitos (…). 2.- El acceso universal a las tecnologías de información y comunicación. 3.- La creación de medios de comunicación social, y al acceso en igualdad de condiciones (…). 4.- El acceso y uso de todas las formas de comunicación visual, auditiva, sensorial (…). 5.- Integrar los espacios de participación previstos en la Constitución en el campo de la comunicación.
Art. 66. Se reconoce y garantiza a las personas:	1.- La protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter (…). 2.- La inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley (…).

Art. 313.	El Estado se reserva el derecho de administrar, regular, controlar y gestionar los sectores estratégicos, de conformidad con los principios de sostenibilidad ambiental, precaución, prevención y eficiencia. Los sectores estratégicos, (…) son aquellos que por su transcendencia y magnitud tienen decisiva influencia económica, social, política o ambiental, (…).
Art. 393.	El Estado garantizará la seguridad humana a través de políticas y acciones integradas, para asegurar la convivencia pacífica de las personas (…).

Fuente: CRE (2008) y Pozo (2022). Autor: Guamán (2023)

Del mismo modo, el COIP (2014) tipifica un conjunto de delitos que limitan el ejercicio de los derechos de las personas con el propósito de garantizar la seguridad en el contexto de los sistemas tecnológicos, como se puede evidenciar en la Tabla 2. Consisten en normas jurídicas de carácter punitivo, en el cual el Estado ecuatoriano ejerce el *ius puniendi* para promover y garantizar la cultura de paz, el buen vivir o *sumak kawsay* y la seguridad en el ciberespacio.

Tabla 2. COIP garantiza la seguridad y protección de las personas frente a delitos informáticos

Art. 103. Pornografía con utilización de niños, niñas o adolescentes.	La persona que fotografíe, filme, grabe, produzca, transmita o edite materiales visuales, audiovisuales, informáticos, electrónicos (…) será sancionada con pena privativa de libertad de trece a dieciséis años, y en un caso de abuso de veintidós a veintiséis años.
Art. 104. Comercialización de pornografía con utilización de niños, niñas o adolescentes.	La persona que publicite, compre, posea, porte, transmita, descargue, almacene, importe, exporte o venda, por cualquier media, (…) será sancionada con pena privativa de libertad de uno a tres años.
Art. 178. Violación de la intimidad.	La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, (…) será sancionada con pena privativa de libertad de uno a tres años.
Art. 190. Apropiación fraudulenta por medios electrónicos.	La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años.
Art. 194. Comercialización ilícita de terminales móviles.	La persona que comercialice terminales móviles con violación de las disposiciones y procedimientos previstos en la normativa emitida por la autoridad competente de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años.
Art. 229. Revelación ilegal de base de datos.	La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, (…), será sancionada con pena privativa de libertad de unos a tres años (…).

Art. 230. Intercepción ilegal de datos.	Será sancionado con pena privativa de libertad de tres a cinco años (…).
Art. 231. Transferencia electrónica de activo patrimonial.	La persona que, con ánimo de lucro, altere, manipule (…) será sancionada con pena privativa de libertad de tres a cinco años.
Art. 234. Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.	La persona que sin autorización acceda en todo o en parte a un sistema informático (…) para explotar ilegítimamente el acceso logrado, modificar un portal web, (…) será sancionada con la pena privativa de la libertad de tres a cinco años.

Fuente: COIP (2014) y Pozo (2022). Autor: Guamán (2023)

Una normativa que regula las nuevas tecnologías, con precisión es la Ley de Comercio Electrónico, Firmas y Mensajes de Datos del año 2002, considerando que el uso de sistemas de información y de redes electrónicas, incluida la internet, ha adquirido importancia para el desarrollo del comercio y la producción, permitiendo la realización y concreción de múltiples negocios de trascendental importancia, tanto para el sector público como para el sector privado. Por lo que es indispensable que el Estado ecuatoriano cuente con herramientas jurídicas que le permitan el uso de los servicios electrónicos, incluido el comercio electrónico y acceder con mayor facilidad a la cada vez más compleja red de los negocios internacionales, como se evidencia en la Tabla 3. En la cual Ecuador se basó en el modelo de ley establecido por la Comisión de las Naciones Unidas para una Ley Comercial Internacional (UNCITRAL).

Tabla 3. Ley de Comercio Electrónico, Firmas y Mensajes de Datos (2002) garantiza la seguridad y protección de las personas frente a delitos informáticos

Art. 2.- Reconocimiento jurídico de los mensajes de datos.	Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta ley y su reglamento.
Art. 4.- Propiedad intelectual.	Los mensajes de datos estarán sometidos a las leyes, reglamentos y acuerdos internacionales relativos a la propiedad intelectual.
Art. 5.- Confidencialidad y reserva.	Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta ley y demás normas que rigen la materia.
Art. 9.- Protección de datos.	Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros. La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución.
Art. 50.- Información al consumidor.	En la prestación de servicios electrónicos en el Ecuador, el consumidor deberá estar suficientemente informado de sus derechos y obligaciones, de

	conformidad con lo previsto en la Ley Orgánica de Defensa del Consumidor y su Reglamento. Cuando se tratare de bienes o servicios a ser adquiridos, usados o empleados por medios electrónicos, el oferente deberá informar sobre todos los requisitos, condiciones y restricciones para que el consumidor pueda adquirir y hacer uso de los bienes o servicios promocionados.
Art. 57.- Infracciones informáticas.	Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley.

Fuente: Ley de Comercio Electrónico, Firmas y Mensajes de Datos (2002). Autor: Guamán (2023)

El Estado ecuatoriano consideró indispensable proveer a los servicios de telecomunicaciones de un marco legal acorde con la importancia, complejidad, magnitud, tecnología y especialidad de dichos servicios, de suerte que se pueda desarrollar estaactividad con criterios de gestión empresarial y beneficio social; así como asegurar una adecuada regulación y expansión de los sistemas radioeléctricos y servicios de telecomunicaciones a la comunidad y mejorar permanentemente la prestación de los serviciosexistentes, de acuerdo a las necesidades del desarrollo social y económico del país, como sepuede observar en la Tabla 4.

Tabla 4. Ley Especial de Telecomunicaciones (2011) garantiza la seguridad y protección de las personas frente a delitos informáticos

Art. 11.- Uso prohibido.	Es prohibido usar los medios de telecomunicación contra la seguridad del Estado, el orden público, la moral y las buenas costumbres. La contravención a esta disposición será sancionada de conformidad con el Código Penal y más leyes pertinentes.
Art. 14.- Derecho al secreto de las telecomunicaciones.	El Estado garantiza el derecho al secreto y a la privacidad de las telecomunicaciones. Es prohibido a terceras personas interceptar, interferir, publicar o divulgar sin consentimiento de las partes la información cursada mediante los servicios de telecomunicaciones.
Art. 25.- Derecho al servicio.	Todas las personas naturales o jurídicas, ecuatorianas o extranjeras, tienen el derecho a utilizar los servicios públicos de telecomunicaciones condicionado a las normas establecidas en los reglamentos y al pago de las tasas y tarifas respectivas. Las empresas legalmente autorizadas establecerán los mecanismos necesarios para garantizar el ejercicio de los derechos de los usuarios.
Art. 27.- Delitos contra las telecomunicaciones.	Los delitos cometidos contra los medios y servicios de telecomunicaciones serán los tipificados en el Código Penal y serán sancionados de conformidad con lo dispuesto en dicho código.

Fuente: Ley Especial de Telecomunicaciones (2011). Autor: Guamán (2023)

El Estado ecuatoriano en continuidad con estas estrategias informáticas, en el año 2011 emite la *Estrategia Ecuador Digital*, por parte del Ministerio de Telecomunicaciones y

de la Sociedad de la Información (en adelante MINTEL), con el propósito de plantear políticas públicas sectoriales que permitan que las tecnologías de la información y comunicación sean utilizadas de manera confiable y efectiva, en correspondencia con el desarrollo social, productivo y solidario del país. En el 2021 publica Programas de Acción en seguimiento de estas estrategias.

En mayo de 2021, la Asamblea Nacional del Ecuador, promulga la *Ley Orgánica de Protección de Datos Personales*, de importancia significativa en esta regulación nacional contra los delitos informáticos; el contar una Ley de Protección de Datos Personales permitirá que las instituciones y las empresas privadas, cuyo giro de negocios son los datos (bases de datos), tengan los criterios para saber qué medidas tecnológicas y organizativas deben implementar, con la finalidad de que los datos que poseen estén adecuadamente resguardados y usados.

En el año 2022 el gobierno nacional emite la *Política de Datos Abiertos* que tiene como objetivo implementar los datos abiertos en la Función Ejecutiva para fortalecer la participación ciudadana, la transparencia gubernamental, mejorar la eficiencia en la gestión pública, promover la investigación, el emprendimiento y la innovación en la sociedad.

A *nivel internacional*, es indispensable, también, analizar la legislación con la cual Ecuador tiene consenso en las valoraciones político jurídicas de los conflictos que se derivan del uso indebido de medios electrónicos, lo que ha permitido que la normativa penal de los Estados sea modificada y adaptada a estas disposiciones internacionales.

Hubo la necesidad de aplicar y armonizar en el contexto internacional las leyes penales, con la finalidad de combatir el uso indebido de los medios informáticos, por lo que la Organización de Cooperación y Desarrollo Económico (en adelante OCDE) en 1983. En 1986 esta misma Organización emitió un Informe denominado Delitos de Informática; Análisis de la normativa jurídica, en la que se compila la normativa vigente para la época y se proponen reformas en las legislaciones internas de los países miembros, sugiriendo las conductas delictivas que serán objeto de sanción, como el fraude, la apropiación fraudulenta, la falsificación informática, la alteración de datos y programas de computadoras, entre otros.

Ante este escenario, el Consejo de Europa aprueba en 1989 la Recomendación R (89)9 sobre Delitos Informáticos, adoptada por el Comité de Ministros del Consejo de Europa, con el propósito de mantener una legislación homogénea frente a la realidad que se vive, haciendo énfasis en la delincuencia digital, como lo señala Sempertegui (2022). Más adelante, la Organización de Naciones Unidas (en adelante ONU) en la Habana celebró el Octavo Congreso sobre Prevención del Delito y Justicia Penal, en el que consideró a la ciberdelincuencia un flagelo producto del aumento del uso de datos en la economía. Campos (2019) señala que

En el año 2001 el Consejo de Europa elaboró el Convenio de Budapest sobre la ciberdelincuencia, en él se establecen normas de cooperación internacional para realizar procesos penales que ayuden a combatir los delitos informáticos; pues el avance de la tecnología ha permitido que los delincuentes informáticos inventen nuevas formas de delinquir. Según estimaciones de LACNIC (2022), el organismo que maneja el Registro de Direcciones de Internet para América Latina y Caribe, el ciber crimen le cuesta a nuestra región alrededor de 90.000 millones de dólares al año.

6.2. Consecuencias de la vulneración de los derechos de las personas por la comisión de estos delitos informáticos

Bien es conocido que, a partir de la década de los años 80 del siglo pasado, con la entrada de la tecnología informática y digital a todos los aspectos de la vida social, familiar e individual, comenzaron a surgir nuevos riesgos personales y sociales automáticos, anónimos y descentralizados que demandaron el estudio de los delitos informáticos, convertidos en un nuevo paradigma de criminalidad, que vulnera varios derechos de los usuarios. Una necesidad que se ha incrementado de modo sustancial durante la pandemia del Covid-19, debido al modelo virtual que se ha impuesto en la vida cotidiana. Este cambio significativo que, sin duda, ha incrementado la vulnerabilidad de las personas y las ha hecho dependientes a la tecnología, lo que ha provocado el aumento de la ciberdelincuencia, en especial, aquellas conductas punibles que lesionan o ponen en peligro la intimidad personal y el patrimonio económico.

Algunas modalidades de estas conductas punibles son, como señalan Ballesteros y Hernández (2022),

> las estafas realizadas por medios informáticos (ventas fraudulentas en páginas falsas, ofrecimientos engañosos en línea, inversiones o estafas piramidales online, casinos o loterías arregladas, etc.), la transferencia no consentida de activos patrimoniales (incluyendo monedas virtuales o "puntos" de supermercados o aerolíneas), las defraudaciones y el tráfico ilícito de datos personales (el *fishing* o la violación de datos), los delitos de intrusión o acceso abusivo a los sistema informáticos –piénsese en las intrusiones en plataformas virtuales como Zoom o *Microsoft Teams*, que han afectado la intimidad de los usuarios educativos–, el mercadeo ilícito de productos a través de internet, los delitos de obstaculización de datos o sistemas informáticos (sabotajes o denegaciones de servicios informáticos), entre otros comportamientos que lesionan de manera grave los bienes jurídicos. De allí que sea necesario promover la adecuada investigación, judicialización y sanción de estos delitos, no solo con el fin de prevenir su comisión futura, sino también para proteger la seguridad de la información, los datos y las infraestructuras informáticas críticas. (p. 19)

Es decir, cuando una persona adquiere un dispositivo móvil o una computadora no solo adquiere los servicios que ofrece el dispositivo, sino que también busca la protección de los datos contenidos en él y la defensa de su confidencialidad. Igualmente, se protege su disponibilidad, es decir, que el ciber usuario pueda acceder según su conveniencia –de manera directa o remota– a un equipo conectado a redes de telecomunicaciones y usar o tratar la información almacenada allí, sin ninguna clase de obstáculo o impedimento grave, ilegítimo o no consentido.

Dentro de este contexto, es fundamental para el ciber usuario que el sistema informático, los datos y la información permanezcan íntegros y funcionen en todo momento de manera correcta, sin ser vulnerados de manera violenta o abusiva por parte de terceros que pretendan modificarlos, manipularlos o disminuir su calidad con el propósito de lesionar otros bienes jurídicos como la intimidad personal. Finalmente, es importante garantizar que el sujeto conserve la capacidad de buscar información en el dispositivo o en la nube, ante la

enorme cantidad de información que se conserva en estos medios. La seguridad de todas estas situaciones garantiza de manera adecuada la seguridad colectiva e individual de la interacción tecnológica.

Por lo que se hace necesario compartir las estadísticas, más recientes, de los delitos cibernéticos en Ecuador en los últimos cinco años, como se puede apreciar en la Tabla 5, para contrarrestar el déficit de estadísticas criminales confiables que reflejan la ocurrencia y los efectos del ciber crimen en la sociedad (efectos económicos, sexuales, de protección de datos, contra la intimidad, violaciones a los derechos morales y patrimoniales de autor, etc.).

Tabla 5. Estadística delitos cibernéticos en Ecuador. Últimos 5 años.

Art. COIP	Tipo Penal/Art.	2017	2018	2019	2020	2021	TOTAL
103	Pornografía con utilización de niñas, niños o adolescentes	203	104	81	113	95	496
104	Comercialización de pornografía con utilización de niñas, niños o adolescentes	26	9	17	18	15	85
173	Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	258	202	185	152	152	829
174	Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos	12	14	16	7	7	56
178	Violación a la intimidad	1160	1062	2038	1985	1346	9.091
186	Estafa	13.911	14.268	16.918	18.415	16.272	79.784
188	Aprovechamiento ilícito de servicios públicos	102	130	194	99	72	597
190	Apropiación fraudulenta por medios electrónicos	959	1448	1744	2280	3952	10.393
192	Intercambio, comercialización o compra de información de equipos terminales móviles	-	-	-	1	1	2
193	Reemplazo de identificación de terminales móviles	4	2	-	3	-	9
194	Comercialización ilícita de terminales móviles	24	14	7	285	10	340
195	Infraestructura ilícita	-	5	7	-	-	12
211	Supresión, alteración o suposición de la identidad y estado civil	52	81	54	23	28	238
229	Revelación ilegal de base de datos	22	44	34	30	23	153
230	Interceptación ilegal de datos	63	41	86	73	35	298
231	Transferencia electrónica de activo patrimonial	54	37	50	75	170	387
232	Ataque a la integridad de sistemas informáticos	85	88	111	95	86	463
233	Delitos contra la información pública reservada legalmente	14	12	5	5	4	40
234	Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	218	236	262	295	274	1.265
366	Terrorismo	12	120	65	13	17	227
Total general por años		**17.480**	**18.914**	**21.834**	**23.968**	**22.569**	**104.765**

Fuente: Sistema Integrado de Actuaciones Fiscales (SIAF) y Fiscalía General del Estado (2022).

Este cuadro estadístico evidencia que los ataques de los ciberdelincuentes y ciber mafias son bastante recurrentes en el país, siendo los más frecuentes la estafa digital y la apropiación fraudulenta por medios electrónicos que traen como consecuencia la vulneración de derechos de los usuarios como el derecho a la intimidad, derechos morales y patrimoniales de autor, derecho al buen vivir, derecho a la seguridad colectiva e individual, entre otros.

6.3. Características esenciales de la apropiación fraudulenta por medios electrónicos en la provincia de Imbabura con el fin de conocer y erradicar en lapráctica este tipo penal digital

Es de advertir que, la informática en sus comienzos se consideraba un servicio inminente para lograr el desarrollo de la sociedad; sin embargo, con el devenir de los años, el uso de los medios electrónicos ha generado un espacio, bastante amplio, para que la delincuencia actúe a sus anchas, con pocas posibilidades, de ser perseguidos por la justicia ordinaria, debido a las habilidades y manera, muy particular, de actuación por parte de estos delincuentes de cuello blanco.

Se pueden desglosar varias características relevantes de este delito, de acuerdo a Rodríguez (2020), que toma en cuenta al autor Téllez-Valdés:

a) Es una conducta criminógena de cuello blanco, se refiere a que únicamente personas con conocimientos técnicos en el área de la informática pueden cometerlos;
b) Es una acción ocupacional, cuando el sujeto se encuentra trabajando.
c) Es una acción de oportunidad, el sujeto lo realiza aprovechando una ocasión creada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
d) Provocan serias pérdidas económicas: quienes los realizan tienen una intención de beneficiarse económicamente, produciendo un deterioro patrimonial al sujeto pasivo.

e) Ofrecen facilidades de tiempo y espacio: susceptibles a ser realizados en tan solo segundos y sin necesidad que el sujeto se encuentre físicamente puede consumarse el hecho.
f) Son muchos los casos y pocas las denuncias: muchas veces, por vacíos jurídicos, o por la dificultad probatoria.
g) Presentan grandes dificultades para su comprobación: el sujeto no suele dejar evidencias.
h) Son imprudenciales: se los cometen por descuido, con respecto a esto se debe discrepar porque el sujeto no actúa imprudentemente, sino al contrario con voluntad y conocimiento del hecho.
i) Ofrecen facilidades para su comisión a los menores de edad: se ven en la red tutoriales de cómo pueden *hackear* cuentas de una *app store*, por ejemplo, y está al alcance de todos inclusive los niños y adolescentes.
j) Tienden a proliferar cada vez más: la tecnología avanza y nuevas formas de atacar a esta tecnología y hacer mal uso de la misma aparecen, por lo que se hace necesario una regulación.
k) Por el momento siguen siendo ilícitos manifiestamente impunes ante la ley. (p. 13)

De igual manera se pronuncia Sempertegui (2022), que este delito se caracteriza por la rapidez en que se comete, por la distancia geográfica que pueda existir entre el lugar de cometimiento de la acción ilícita y el de la producción de los resultados o efectos jurídicos del delito; otra característica, es la dificultad para descubrir y perseguir a sus autores, quienes, con gran habilidad, borrar las huellas o alteran programas y datos, sin dejar rastro, asegurando su total impunidad.

6.3.1. Bien jurídico protegido en los delitos por medios electrónicos

El bien jurídico protegido es un elemento relevante para el derecho penal moderno, pues su afectación da lugar al castigo punitivo, por parte del Estado, de las conductas delictuales que ponen en riesgo, en peligro o lesionan un bien. Esto da lugar a que se generen

controversias entre los autores penales, sobre lo que se considera bien jurídico. Por lo que se analizan algunas de ellas:

El maestro italiano, considerado el abanderado del garantismo penal, Ferrajoli (2006) señala que "la lesión del bien jurídico protegido, debe ser condición necesaria, aunque nunca suficiente para justificar su prohibición y punición como delito" (p. 72). En este mismo sentido, Roxin (1997) manifiesta que "el bien jurídico, por tanto, es el bien ideal que se incorpora en el concreto objeto de ataque; y es lesionable sólo dañando los respectivos objetos individuales de la acción" (p. 63).

Del mismo modo Zaffaroni (1989) enseña que "el bien jurídico penalmente tutelado es la relación de disponibilidad de un individuo con su objeto, protegida por el Estado, que revela su interés mediante la tipificación penal de conductas que le afectan" (p. 289). Según lo cual, la comisión de delitos informáticos, da lugar a la afectación de diversos bienes jurídicos protegidos.

Por lo que Sempertegui (2022) afirma que "de forma general que el bien jurídico protegido en los delitos informáticos es la *información*, que, de acuerdo con el tipo penal, debe ser considerada en diversas formas, de modo que, su lesión trasciende a bienes jurídicos secundarios y tradicionalmente protegidos como son: la propiedad, el patrimonio, la seguridad, la intimidad y confidencialidad" (p. 14).

El patrimonio y la propiedad de una persona es el bien jurídico protegido por el Derecho, debido a que, al configurarse un delito informático de apropiación ilícita, se vulneran los derechos de propiedad, de que goza una persona; no obstante, por la gravedad de los mismos, puede llegarse a lesionar otros bienes jurídicos protegidos como el derecho a la intimidad personal, y la seguridad nacional. También determinaron que, el objeto material del delito informático consiste en bienes, derechos o valores de naturaleza digital, contenidos dentro de los sistemas informáticos.

Además de lo anterior, Rodríguez (2020) indica que, "existen varios criterios en que se coincide en establecer como el bien jurídico protegido de los delitos informáticos es la *información* mientras que, en otros casos, se habla de que este bien jurídico sería la *libertad informática"* (p. 9).

Desde esta perspectiva, Chitalogro (2022) mantiene que "al ser la seguridad informática uno de los bienes jurídico protegidos, nos lleva a cuestionarnos si este tipo penal debería constar en los delitos contra la seguridad de los activos de los sistemas de información y comunicación dado que en el primer apartado la realización de ciertas acciones típicas afecta a los sistemas informáticos y en el segundo apartado ya se vulnera como tal la seguridad de los sistemas informáticos" (p. 58). Por lo que se puede señalar que el bien jurídico protegido de acuerdo con la CRE es la llamada *libertad de informática* que consiste, como expresión de la libertad del individuo, en el derecho de utilizar lícita y libremente, con los límites constitucionales y legales la tecnología informática.

6.4. Entrevista realizada a Jueces de la Unidad Judicial de Multicompetente del Cantón Antonio Ante y del Juzgado Tercero de Garantías Penales, provincia de Imbabura

Pregunta No. 1	¿Cómo define al delito de apropiación fraudulenta de medios electrónicos?
Luis Santiago Vallejo Salazar, Juez de la Unidad Judicial Multicompetente de Atuntaqui**.**	Este delito de fraude a través de medios electrónicos se presenta como la persona implicada en el inadecuado uso de la tecnología, sus técnicas y funciones utilizadas para apropiarse de un bien ajeno.
Alcívar Rodolfo Tulcanazo Sarabino, Juez de la Unidad Judicial Penal de Ibarra	Se define como el comportamiento con dolo en perjuicio de una tercera persona mediante la utilización de cualquier medio electrónico, con el fin de realizar un acto sin consentimiento o la autorización legal.
María Dolores Echeverría Vásquez, Jueza Tribunal de Garantías Penales de Imbabura	Este mecanismo comprende un sistema de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de esta o de un tercero.
Segundo Méndez Criollo, Juez de la Unidad Judicial Multicompetente de Atuntaqui	La apropiación por medios electrónicos se define como el medio de apropiación fraudulentamente en donde se vea alterado o modificado datos electrónicos para obtener beneficios económicos de ello.

Fuente: Entrevistados (2022). Guamán, (2023).

Análisis

Se puede argumentar que la apropiación fraudulenta por medios electrónicos ocurre cuando un tercer priva de su dinero, capital o altera información financiera de otra persona a través de prácticas engañosas o prácticas ilegales. Esto se puede hacer a través de una variedad de métodos, como el robo de información, actos delictivos cometidos en línea imágenes, grabaciones, suplantación mediante correo electrónico, robo de identidad o el fraude.

Pregunta No. 2	Dentro de la actual legislación sobre el delito de apropiación fraudulenta por medios electrónicos ¿Cómo afecta a los derechos personales de cada individuo?
Luis Santiago Vallejo Salazar, Juez de la Unidad Judicial Multicompetente de Atuntaqui	Dentro de un proceso judicial como la apropiación de medios electrónicos cuando existe fraude a gran escala, toma en perjuicio del individuo como la salud física y mental, la integridad moral y el respeto por las libertades individuales y la privacidad al verse afectados por este delito.
Alcívar Rodolfo Tulcanazo Sarabino, Juez de la Unidad Judicial Penal de Ibarra	El proceso se encuentra ajustado a los preceptos constitucionales y legales inherentes, algunos derechos incluyen el derecho a la seguridad personal.
María Dolores Echeverría Vásquez, Jueza Tribunal de Garantías Penales de Imbabura	Si medimos la importancia de un documento de derechos humanos por su alcance, se debe fundamentar en la condición de individuo, que en mencionado delito es la integridad personal y la seguridad jurídica que en ciertos casos se ve vulnerado por los mismos trabajadores de la entidad bancaria.
Segundo Méndez Criollo, Juez de la Unidad Judicial Multicompetente de Atuntaqui	Afecta directamente al individuo y su familia puesto que es un medio importante de protección para todos nosotros, especialmente, para aquellos que pueden enfrentar este delito.

Fuente: Entrevistados (2022). Guamán, (2023).

Análisis

Lo que proporciona este delito es la vulneración de la privacidad de las personas y la seguridad de sus datos, mensajes; el Estado es el encargado de proteger a las personas de los

daños resultantes de actividades delictivas realizadas a través de Internet. Para lo cual, las respuestas gubernamentales frente a la apropiación fraudulenta de medios electrónicos, la mayor para quedarse impunes, ineficaces o desproporcionadas, lo que vulnera derechos.

Pregunta No. 3	Dentro del ascenso del mencionado delito, ¿cuándo hay suficiente evidencia para establecer una relación causal entre los autores del delito y la entidad bancaria?
Luis Santiago Vallejo Salazar, Juez de la Unidad Judicial Multicompetente de Atuntaqui	Yo creo que los factores de empuje para la responsabilidad del banco y sobre las tendencias en este delito contra la propiedad a través de medios electrónicos si incluye el papel de algunos de sus miembros, aclaro que no en todas las entidades bancarias, pero en las líderes sí, ya que se ven involucrados en trabajos inestables.
Alcívar Rodolfo Tulcanazo Sarabino, Juez de la Unidad Judicial Penal de Ibarra	Si y no, primero porque como se ha evidenciado en los últimos meses ha habido un incremento en la modalidad para cometer este delito, ¿Cómo saben si la cantidad es grande o no?, es una pregunta que va a la par con muchas personas, justamente van hacía estas personas. Y no, porque no generalizo, simplemente hay más seguridad a la hora de mantener el servicio y protección de sus bienes.
María Dolores Echeverría Vásquez, Jueza Tribunal de Garantías Penales de Imbabura	Pienso que la misma delincuencia puede permanecer dentro del banco, ya que no existe un control en sí uniforme, es decir, los guardias lo único que realizan es el manejo de filas y que no haya aglomeraciones, que no haya peleas entre el servidor privado y quien retira el dinero, pero que haya complicidad dentro del banco es posible, por ejemplo, en el uso de tarjetas de crédito, cuando hay nuevos usuarios, a través de llamadas las efectúan pidiendo los datos de mencionada tarjeta.
Segundo Méndez Criollo, Juez de la Unidad Judicial Multicompetente de Atuntaqui	Existe mucho personal bancario que es difícil sondear, pero cada banco es quien debe ante todo primar por la seguridad personal de cada cliente, el robo de identidad y el fraude con tarjetas de crédito son delitos estrechamente relacionados con quienes han denunciado sobre este delito.

Fuente: Entrevistados (2022). Guamán, (2023).

Análisis

Los procedimientos de seguridad de algunas entidades bancarias no cumplen con el estándar, sin embargo, también son responsables de realizar un procedimiento legal atribuible los agentes del orden público, fiscales y jueces, que son los responsables de la prevención, mitigación, detección, investigación, enjuiciamiento y adjudicación de la apropiación fraudulenta de medios electrónicos.

Pregunta No. 4	¿Cuándo existe vulnerabilidad probable en el delito de apropiación fraudulenta de medios electrónicos?, ¿Cómo se logra sancionar este delito en el Código Orgánico Integral Penal?
Luis Santiago Vallejo Salazar, Juez de la Unidad Judicial Multicompetente de Atuntaqui	El delito de apropiación fraudulenta por medios electrónicos es tipificado por el Código Orgánico Integral Penal Art. 190, por lo que sanciona de uno a tres años, se ven vulnerados la confidencialidad y la integridad, entre otros.
Alcivar Rodolfo Tulcanazo Sarabino, Juez de la Unidad Judicial Penal de Ibarra	Como todos los procedimientos este delito puede perpetrarse únicamente para obtener e interferir con el acceso a los sistemas en línea, servicios y datos. Este delito es sancionado de uno a tres años, según corresponda.
María Dolores Echeverría Vásquez, Jueza Tribunal de Garantías Penales de Imbabura	Según el Código Orgánico Integral Penal, en su Art. 190, por lo que la apropiación fraudulenta por medios electrónicos también se vevulnerada al producir, poseer o distribuir el usoindebido de información como contraseñas, códigos de acceso y otros datos que permiten a las personas obtener acceso ilegal.
Segundo Méndez Criollo, Juez de la Unidad Judicial Multicompetente de Atuntaqui	Esta conducta ilícita se encuentra tipificada en el Art. 190 del Código Orgánico Integral Penal, infringe la privacidad de las personas y la seguridad de sus datos.

Fuente: Entrevistados (2022). Guamán, (2023).

Análisis

El Artículo 190 del Código Orgánico Integral Penal sobre la apropiación fraudulenta por medios electrónicos ocurre cuando los perpetradores están familiarizados con el

funcionamiento interno de entidades bancarias, envían correos electrónicos dirigidos a los miembros de estas entidades para engañarlos para que revelen información, suplantación de identidad, sancionada con pena privativa de libertad de uno a tres años.

Pregunta No. 5	El derecho a la intimidad es afectado por el delito de apropiación fraudulenta por medios electrónicos, como ente sancionador, ¿cómo actúa el sistema penal ecuatoriano al momento de reparación integral a la víctima?
Luis Santiago Vallejo Salazar, Juez de la Unidad Judicial Multicompetente de Atuntaqui	Los modelos de reparación pueden aplicarse en este delito, porque busca el resarcimiento de un derecho vulnerado, por ejemplo, la explotación infantil en línea a través de fotografías y el robo fraudulento en línea.
Alcivar Rodolfo Tulcanazo Sarabino, Juez de la Unidad Judicial Penal de Ibarra	Este delito ha tenido un rápido crecimiento en la proliferación de la apropiación fraudulenta de medios electrónicos, en donde permite que cualquier persona con acceso a internet se comunique e intercambie información de una manera altamente insegura provocando vulneración en su derecho a la intimidad, por lo que el Estado no debe dejar impunidad de este delito y el justo derecho de la víctima a ser reparada integralmente después de que sus derechos fueron violentados de forma arbitraria.
María Dolores Echeverría Vásquez, Jueza Tribunal de Garantías Penales de Imbabura	El juzgador es el encargado de analizar y ordenar la práctica de la que fuese más adecuada según el derecho vulnerado, buscando cubrir totalmente las necesidades de las víctimas.
Segundo Méndez Criollo, Juez de la Unidad Judicial Multicompetente de Atuntaqui	La protección de los datos personales, en particular los que están involucrados en medios electrónicos, es de fundamental importancia para que una persona disfrute de su derecho a la intimidad, y si se ven afectados se recurra a los principios y directrices básicos mediante la restitución o compensación según sea el tipo de caso.

Fuente: Entrevistados (2022). Guamán, (2023).

Análisis

La reparación integral por graves vulneraciones a los derechos humanos no son cuestiones que dependan de la voluntad política, son claras obligaciones jurídicas, puesto que al verse afectado el derecho a la intimidad siendo este un derecho humano fundamental reconocido por la Constitución de la República del Ecuador.

Pregunta No. 6	¿Cómo define a la seguridad informática?
Luis Santiago Vallejo Salazar, Juez de la Unidad Judicial Multicompetente de Atuntaqui	La seguridad en la información es definida como la protección de los sistemas informáticos y la información contra daños, robos y uso no autorizado.
Alcivar Rodolfo Tulcanazo Sarabino, Juez de la Unidad Judicial Penal de Ibarra	Es el proceso de prevenir y detectar el uso no autorizado de un sistema informático ya sea de alguna persona, empresas, es decir, comprende un todo.
María Dolores Echeverría Vásquez, Jueza Tribunal de Garantías Penales de Imbabura	La seguridad informática se puede definir como los controles que se implementan para brindar confidencialidad, integridad y disponibilidad para todos los componentes de los sistemas informáticos y de cada individuo.
Segundo Méndez Criollo, Juez de la Unidad Judicial Multicompetente de Atuntaqui	La seguridad informática es la protección que se configura para los sistemas informáticos para evita el acceso no autorizado, el robo o el uso indebido de información confidencial y de uso privado.

Fuente: Entrevistados (2022). Guamán, (2023).

Análisis:

Se entiende que la seguridad informática se refiere a la protección del hardware de una computadora y los datos que esta contiene, pudiendo implementar contraseñas, cifrado y negando el acceso físico a la ubicación de cada sistema; si bien las medidas de seguridad no garantizan que los datos no se vean comprometidos, los pasos adicionales ciertamente pueden ayudar a evitar el acceso y la adquisición de datos no autorizados.

Pregunta No. 7	Defina confidencialidad, integridad y disponibilidad sobre la apropiación fraudulenta por medios electrónicos.
Luis Santiago Vallejo Salazar, Juez de la Unidad Judicial Multicompetente de Atuntaqui	A raíz del creciente delito sobre la apropiación, es que se puede reflexionar sobre la importancia de las medidas de prevención para evitar futuros incidentes. Como principio general del control interno, sabemos que los controles preventivos son siempre preferibles a los controles correctivos y estas medidas de control aplicadas a la protección de datos no son la excepción, en donde debe primar la integridad y seguridad de cada persona.
Alcivar Rodolfo Tulcanazo Sarabino, Juez de la Unidad Judicial Penal de Ibarra	Para las personas hoy en día la tecnología, en general, se presenta como una puerta abierta al mundo en su entorno personal y, en muchos casos, fácil de usar, con grandes accesos a perpetrar la confidencialidad.
María Dolores Echeverría Vásquez, Jueza Tribunal de Garantías Penales de Imbabura	Los estándares de seguridad sobre la información también pueden utilizarse con muy poca metodología, es decir, que es fácil su desarrollo mediante, un mensaje en redes sociales, llamadas para pedir números de tarjeta de crédito, aunque las aplicaciones parecen seguras los controles para autenticación y autorización, suelen ser efectivos, es de conocimiento que las mismas venden la información de sus mismos clientes, por ello vulnera el sistema sin resguardar la confidencialidad y seguridad.
Segundo Méndez Criollo, Juez de la Unidad Judicial Multicompetente de Atuntaqui	Esto son conceptos básicos que abordan la integridad, confidencialidad y disponibilidad, que vienen siendo propiedades básicas que preserva la seguridad de la información, manteniendo a la información de manera completa y exacta.

Fuente: Entrevistados (2022). Guamán, (2023).

Análisis

Una de las condiciones fundamentales para que un sistema social funcione, reside en el desarrollo de una estructura que garantice a las personas un ambiente de confianza que procure su estabilidad, sin embargo, estos supuestos se han visto vulnerados a causa de la generalización y masificación del uso del Internet.

La digitalización ha logrado abarcar cada ámbito de la sociedad a una velocidad inatrapable para las gestiones que se encargan de administrarla, lo cual, ha generado en un enorme desafío resultado de la tensión entre la seguridad y la privacidad.

Se procedió a analizar las brechas de seguridad en los sistemas informáticos sobre la privacidad, falsificar la entidad de cada individuo en donde se presenta el resultado del análisis documental referente a las normas legales nacionales e internacionales sobre la apropiación fraudulenta por medios electrónicos, en donde, se ha logrado determinar que en la actualidad el Estado ecuatoriano reconoce y brinda protección de identidad y datos a cada individuo, a fin de evitar la vulneración de derechos humanos.

Se evidencia que, en la Provincia de Imbabura los datos sobre fraude son escasos, por lo que esto ha limitado seriamente el número de estudios sobre el tema gran parte de la investigación sobre los delincuentes fraudulentos se ha basado en datos cualitativos y estudio de caso, actualmente basado en las entrevistas que se realizó con muestras pequeñas.

En cuanto a los profesionales que contribuyeron con el desarrollo de esta investigación, se entrevistaron Jueces Multicompetentes y Abogados en libre ejercicio, quienes dejan entrever que la apropiación fraudulenta por medios electrónicos en donde deben acudir a instancia judicial ante la negativa del banco de reconocer el valor para una reparación integral.

6.5. Discusión

Tanto los autores analizados en el estado del arte como lo entrevistados en este trabajo investigativo, señalan que el verbo rector existente, es el "*de procurar* la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra personando alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones" (Asamblea Nacional, COIP, 2014, Art. 190). Como sostiene Sempertegui (2022), este verbo rector procurar hace referencia a "intentar, pretender, esforzar, emprender, empezar, tratar, proyectar, trabajar, procurar, etc." (p. 48)

Coinciden los autores, como Aparicio-Izurieta (2022), Ballesteros y Hernández (2022), en mencionar que, entre los elementos necesarios para que se configure la comisión

de este delito, está *el fraude*, considerado como el engaño realizado por el autor del delito, con la finalidad de alterar y afectar los sistemas informáticos que permitan, con mayor facilidad, el cometimiento del hecho ilícito.

Para que este delito de apropiación fraudulenta por medios electrónicos sea perseguible y penalmente relevante, es indispensable determinar la tipicidad subjetiva, es decir, establecer su naturaleza dolosa, que implica que el sujeto activo ostente, en eldesarrollo de su conducta, conciencia y voluntad de los elementos delictuales del mismo y así poder ejercer el *ius puniendi* por parte del Estado, como ejercicio de su soberanía.

Esta investigación, permitió debatir sobre varios puntos relativos a este delito, como fue la sanción señalada en el COIP, algunos comentaron ¿es una sanción justa o proporcional, la privación de libertad de uno a tres años? ¿en qué casos se debe aplicar? y ¿en qué casos no se debe aplicar? ¿Las personas víctimas de delitos informáticos que carecen de pruebas físicas, tienen alguna posibilidad de obtener justicia, de obtener la debida reparación integral al daño patrimonial sufrido?

Coinciden los autores como, Morocho (2022), Pozo (2022) y Aparicio-Izurieta (2022), que estos delitos están aumentando considerablemente, debido, entre otras cosas, al progreso de las TIC, en todos los campos de la sociedad y a la poca información de los usuarios al hacer uso de los mismos y el desconocimiento de los graves daños que pueden sufrir al proporcionar datos e información estrictamente confidenciales.

Romero (2018), indica que “mundialmente los ciberataques son el principal riesgo global de origen humano, con diversas consecuencias que casi siempre se traducen en interrupción de servicios, pérdidas económicas o daños a la reputación de la víctima” (p. 12). Lo cual coincide con lo señalado por los entrevistados que, en la mayoría de los casos de apropiación fraudulenta por medios electrónicos, el fin que se persigue es un fin económico, pero también hay algunas que se realizan con fines activistas para obtener información sobre un adversario, otras como acciones integradas en un plan militar.

Los entrevistados coinciden en señalar que el delito de apropiación fraudulenta por medios electrónicos viola la intimidad de los usuarios de medios electrónicos. Al respecto, González (2021) considera que el delito de violación a la intimidad tipificado en el Art. 178

del COIP hace referencia a la grabación u obtención y publicación de información de otra persona sin su autorización y "busca prevenir y combatir la violencia sexual digital y fortalecer la lucha contra los delitos informáticos; sin embargo, el texto final involucra una polémica reforma" (párr. 1-2). Artículo que fue reformado en 2021 dentro del paquete de reformas al COIP.

Al respecto la Fiscalía General del Estado (en adelante FGE) (2021) en un Comunicado hace mención a la reforma recién del Art. 178 COIP, en los siguientes términos:

> Dicha Ley reforma el Art. 178 del COIP y elimina la excepción –que consta en el segundo inciso de la redacción actual– de la comisión del delito a la violación de la intimidad cuando una persona divulga grabaciones de audio y video en las que interviene personalmente, y cuando se trata de información pública, de acuerdo con lo previsto en la Ley.
>
> Esto, de forma evidente, causa un efecto negativo en las investigaciones penales que dirige la FGE, tomando en cuenta que muchas de las evidencias importantes que permiten develar grandes tramas de corrupción, delincuencia organizada y otros tipos penales, se producen y obtienen mediante esta clase de excepciones, contempladas actualmente en la norma penal ecuatoriana. (FGE, 2021, Comunicado)

El Estado ecuatoriano está convocado a velar por la protección de los derechos, como es el derecho a la intimidad; no obstante, ninguna norma debería propender a garantizar la impunidad, más en momentos de tensión social donde la corrupción se erige como uno de los retos de las autoridades.

En la provincia de Imbabura, por ser fronteriza la apropiación fraudulenta por medios electrónicos, abarca diversas formas de cometerla, ya que no cuenta con un solo verbo rector, sino que existe una pluralidad, ya que menciona que se puede lograr por medio de la alteración, manipulación o modificación informática. Se hace necesario mencionar que, la manipulación o modificación a la que hace referencia el Art. 190 del COIP, no precisamente demanda un contacto directo con el computador objeto del ataque; ya que, con el desarrollo de los medios tecnológicos, el cometimiento de este fraude, aquí en la provincia de Imbabura, se puede efectuar sin acceder al computador objeto de ataque.

Las vías más comunes por las que el sujeto activo puede alcanzar un movimiento contable a su favor son, de acuerdo con Chitalogro (2022):

> a. Introducción de datos falsos o engañosos: Conocido como *Data diddling*, principalmente radica en cambiar, eliminar u ocultar los datos de entrada de un sistema, con el propósito de obtener u ocasionar movimientos falsos en transacciones; b. Manipulaciones de programas: Se basa en modificar los protocolos del programa que ya se encuentran en el sistema o en su momento en introducir nuevos programas, con el propósito de alcanzar un beneficio; c. Manipulación de los datos de salida: Este modelo de manipulación "se efectúa en el sistema de salida de datos fijando un objetivo al funcionamiento del sistema informático; d. *Pishing*: Esta manera de estafar consiste en obtener información del sujeto pasivo, así como números de tarjetas de crédito, información de cuentas, contraseñas u otros datos con la ayuda de engaños, con el objeto de apropiarse de bienes, valores o derechos de un tercero; e. Transferencia no consentida: El traspaso al que se hace referencia como elemento de la apropiación fraudulenta por medios electrónicos debe acontecer de forma no consentida, de modo que la presencia del consentimiento autorizado a la transferencia operaría como razón determinante de la exclusión de la tipicidad. (pp. 52-53)

De esta manera, al establecer que se requiere la transferencia no consentida de bienes, valores o derechos para poder evaluar la consumación de este delito patrimonial, deja expresamente establecido que el delito se consuma cuando se genere la pérdida efectiva de los bienes, valores o derechos.

A pesar de que en ciertos tipos penales la legislación ecuatoriana no establece el medio por el cual se realiza la conducta delictual, es diferente respecto al tipo penal de la apropiación fraudulenta por medios electrónicos, dado que es clara al determinar que la apropiación fraudulenta debe ser realizada por medios electrónicos para poder adecuarla al tipo penal establecido en el Art. 190 del COIP, es decir, que si la apropiación fraudulenta no usa como instrumento los medios electrónicos no se estaría frente a la apropiación fraudulenta por medios electrónicos, a pesar de que sigue siendo un delito, no se puede subsumir en este tipo penal específicamente; por ende, se puede considerar que el medio por el que se realiza la apropiación fraudulenta es un condicionante para su sanción.

Además de ello, se requiere en este tipo penal la presencia de los elementos subjetivos, es

decir, aquellos elementos que hacen referencia al sujeto activo de la acción, y al ser elementos que se encuentran en el mundo psíquico del agente son intangibles e inmateriales pero que son perceptibles por medios de los sentidos; estos elementos son caracteres intangibles que exige el tipo penal del agente. En la apropiación fraudulenta debe evidenciarse el dolo y el ánimo de lucro.

El artículo objeto de análisis contiene dos apartados, en el primero se evidencia que el bien jurídico protegido es el patrimonio, puesto que la acción no tiene como objeto afectar directamente la seguridad del sistema informático, sino que estos sistemas son el instrumento o medio por el cual se va a consumar la apropiación; empero, en el segundo apartado, a diferencia del primero se hace referencia a la vulneración de seguridad de sistemas informáticos como el bien jurídico protegido.

Y de lograrse el cometimiento de este delito por el uso de medios electrónicos, el Código Orgánico Integral Penal, sanciona el delito de apropiación fraudulenta por medios electrónicos con una pena privativa de libertad de uno a tres años, permitiendo al Estado ejercer su fuerza punitiva con la intención de restringir la comisión de este delito que va en incremento dentro de la sociedad.

7. CONCLUSIONES

De la investigación realizada se logró determinar las siguientes conclusiones:

1. Al analizar desde la perspectiva tecno-jurídica la apropiación fraudulenta por medios electrónicos en la provincia de Imbabura, a fin de determinar la vulneración de los derechos de las personas, se señala que los delitos informáticos, en esta zona del país, radican, generalmente, en errores y descuidos atribuibles a los propios usuarios de la internet, descuidos en el manejo de equipos electrónicos donde se guardan los datos y claves de acceso, siendo muy frecuente que las víctimas de estos delitos no denuncien este tipo de actuaciones fraudulentas por múltiples razones como falta de pruebas, dificultad en determinar quien o quienes son los sujetos activos del delito; por lo que escasamente reposan dentro del Consejo de la Judicatura expedientes contentivos de este delito informático.

2. Al describir el régimen jurídico nacional e internacional que tipifica y sanciona la apropiación fraudulenta por medios electrónicos en el Ecuador; en primer término, se señala la CRE (2008) como instrumento jurídico garantista de los derechos de las personas, entabla una relación homogénea entre la sociedad, la seguridad de las personas y la información. Del mismo modo, el COIP (2014) tipifica un conjunto de delitos que limitan el ejercicio de los derechos de las personas con el propósito de garantizar la seguridad en el contexto de los sistemas tecnológicos.

3. Una normativa que regula las nuevas tecnologías, con precisión es la Ley de Comercio Electrónico, Firmas y Mensajes de Datos del año 2002. El Estado ecuatoriano en continuidad con estas estrategias informáticas, en el año 2011 emite la Estrategia Ecuador Digital. En mayo de 2021, la Asamblea Nacional del Ecuador, promulga la Ley Orgánica de Protección de Datos Personales. En el año 2022 el gobierno nacional emite la Política de Datos Abiertos, aunada a una normativa internacional contra la ciberdelincuencia, que consisten en normas jurídicas de carácter punitivo, en el cual el Estado ecuatoriano ejerce el *ius puniendi* para

promover y garantizar la cultura de paz, el buen vivir o *sumak kawsay* y la seguridad en el ciberespacio.

4. Al determinar cuáles fueron las consecuencias de la vulneración de los derechos de las personas frente a los ataques de los ciberdelincuentes y ciber mafias derivadas de la estafa digital y la apropiación fraudulenta por medios electrónicos, como las más recurrentes en el país, generan, de manera directa, la vulneración de derechos de los usuarios como el derecho a la intimidad, derechos morales y patrimoniales de autor, derecho al buen vivir, derechos económicos y sexuales, derecho a la seguridad colectiva e individual de la interacción digital, entre otros.

5. En cuanto a las características esenciales de la apropiación fraudulenta por medios electrónicos se encontró la rapidez en que se comete, la distancia geográfica que pueda existir entre el lugar de cometimiento de la acción ilícita y el de la producción de los resultados o efectos jurídicos del delito; otra característica, considerada fue la dificultad para descubrir y perseguir a sus autores, quienes, con gran habilidad, borran las huellas o alteran programas y datos, sin dejar rastro, asegurando su total impunidad. Lo que ha derivado que en la provincia de Imbabura exista carencia en la persecución de la práctica de este tipo penal digital.

8. RECOMENDACIONES

1. Implementar todas las medidas y sanciones establecidas en las leyes ecuatorianas para erradicar esta práctica delictiva en el ciberespacio de los usuarios ecuatorianos, a los fines de proteger nuestros datos e información personal, ya que son uno de los bienes más importantes con los que se cuenta y que dicen mucho del estilo de vida y de la identidad de cada uno.

2. Separar doctrinariamente las características jurídicas de la apropiación fraudulenta por medios electrónicos, en particular la manipulación, alteración o modificación informática de la transferencia no consentida, pues el hecho de que se encuentren normadas en un mismo artículo generó ambigüedad, incertidumbre y poca claridad al momento de imponer sanciones por la ineficiencia material.

3. Instar al manejo de normas técnicas que describan continuamente los delitos informáticos y sus consecuencias, actualizándolos y adaptándolos a la normativa internacional para estar prevenidos frente a los cambios tecnológicos que se generan como la inteligencia artificial y su impacto en la conducta delictual.

4. Brindar mayor publicidad a fin de que estos delitos sean conocidos por los usuarios del ciberespacio y, de esta manera, precautelar los derechos de los ciudadanos y posteriormente sancionar de manera adecuada, siendo necesaria la capacitación de juezas, jueces y fiscales, para estar a la altura de los adelantos tecnológicos.

5. Ofrecer, por parte del Estado ecuatoriano, mayor certeza en la persecución de los autores de este tipo penal digital y poder rastrear cómo y desde donde se comete el delito, lo cual permitiría un seguimiento más efectivo de los autores y cómplices.

9. REFERENCIAS BIBLIOGRAFÍAS

Acosta, M.; Benavides, M.; García, N. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. En *Revista venezolana de Gerencia*, vol. 25, núm. 89, julio 2020, Universidad del Zulia. Recuperado de https://www.redalyc.org/journal/290/29062641023/29062641023.pdf

Acurio, S. (2019). *Manual de manejo de evidencias digitales y entornos informáticos*. Versión 2.0. Quito: Corporación de Estudios y Publicaciones.

Aparicio-Izurieta, V. (2022). Delitos informáticos en Ecuador según el COIP: un análisis documental. En Revista *Sapienza: Intrenational Journal of Interdisciplinary Studies*, vol. 3, N° 1, jan-mar 2022, 1057-1063. Recuperado de https://www.researchgate.net/publication/359868589_Delitos_informaticos_en_Ecuador_segun_el_COIP_un_analisis_documental

Asamblea Nacional Constituyente del Ecuador, (2008) *Constitución de la República del Ecuador*. Montecristi: Registro Oficial número 449 de 20 de octubre de 2008.

Asamblea Nacional del Ecuador. *Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional* (2009) Registro Oficial Suplemento 52 del 22-octubre-2009. Quito. Recuperado de shorturl.at/NOUW1

Asamblea Nacional del Ecuador. (2014). *Código Orgánico Integral Penal*. Registro Oficial Suplemento 180 de 10-feb-2014. Última modificación: 17-feb.-2021.

Asamblea Nacional del Ecuador. (2016) *Código Orgánico de la Función Judicial*. Primer Suplemento del Registro Oficial. Resolución N°01. Quito-Ecuador: Corte Nacional de Justicia del Ecuador.

CEPAL/CAF (Comisión Económica para América Latina y el Caribe/Banco de Desarrollo de América Latina). (2022). Las oportunidades de la digitalización en América Latina frente al COVID-19, Santiago, abril.

Chitalogro, Y. (2022). *Análisis dogmático penal de los delitos de apropiación fraudulenta y estafa cuando son realizados por medios electrónicos en el COIP*. Quito: Universidad Central del Ecuador. Recuperado de http://www.dspace.uce.edu.ec/bitstream/25000/28485/1/FJCES-CD-CHITALOGRO%20YOMAIRA.pdf

Fiscalía General del Estado (2021). Ciberdelitos. Perfil criminológico. En *Revista Científica de Ciencias Jurídicas, Criminología y Seguridad.* Quito: Dirección de Estudios Penales. Recuperado de https://www.fiscalia.gob.ec/pdf/politica-criminal/Ciberdelitos-Perfil-Criminologico.pdf

Fiscalía General del Estado. (2021). Comunicado, Recuperado de https://twitter.com/FiscaliaEcuador/status/1390855785199149062

Herrera, C. (2018). *Hacia una correcta hermenéutica penal: Delitos informáticos vs. Delitos electrónicos.* Universidad de Cuenca. Recuperado de https://dspace.ucuenca.edu.ec/bitstream/123456789/2673/1/tm4391.pdf

López, F. S. (2020). Detección de fraude en pagos electrónicos mediante aprendizaje supervisado y no supervisado. *Conferencia mundial sobre sistemas y tecnologías de la información* (págs. 88-89). Bogotá: Slice.

Morocho, G. (2022) I*ncidencia del delito de estafa a través de redes sociales, año 2017-2020, cantón La Libertad*. Ecuador: Universidad Estatal Península de Santa Elena. Recuperado de https://repositorio.upse.edu.ec/bitstream/46000/8820/1/UPSE-TDR-2022-0064.pdf

Naranjo, V.; Mendoza, J.; Alonso, E.; Hinojosa, J. (2020) Informática criminalística: una especialidad en desarrollo. En *Revista Opinión Jurídica*, 19(38), enero-junio 2020, 245-257. Recuperado de http://www.scielo.org.co/pdf/ojum/v19n38/1692-2530-ojum-19-38-245.pdf

Organización de Naciones Unidad, en la CEPAL (2022) Tecnologías digitales para un nuevo futuro. Elac-2022. Agenda Digital para América Latina y el Caribe. Recuperado de https://repositorio.cepal.org/bitstream/handle/11362/46816/1/S2000961_es.pdf

Organización para la Cooperación Económica y el Desarrollo. (2021). Boletín de Indicadores Económicos Internacionales, diciembre 2021. Quito: Banco Central del Ecuador. Recuperado de https://contenido.bce.fin.ec/documentos/PublicacionesNotas/BOLETIN412021.pdf

Romero, M. I. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades.* Alicante: Área de Innovación y Desarrollo, S.L.

Sempertegui, M. (2022). *Delitos de apropiación fraudulenta por medios electrónicos bajo la modalidad de phising dentro del marco jurídico ecuatoriano*. Cuenca: Universidad de Azuay. Recuperado de https://dspace.uazuay.edu.ec/bitstream/datos/12380/1/17907.pdf

10. ANEXOS

ENTREVISTA DIRIGIDA A FUNCIONARIOS JUDICIALES

1. ¿Cómo define al delito de apropiación fraudulenta de medios electrónicos?
2. Dentro de la actual legislación sobre el delito de apropiación fraudulenta de medios electrónicos ¿Cómo afecta a los derechos personales de cada individuo?
3. Dentro del ascenso del mencionado delito, ¿Cuándo hay suficiente evidencia para establecer una relación causal entre los autores del delito y la entidad bancaria?
4. Cuando existe vulnerabilidad probable en el delito de apropiación fraudulenta de medios electrónicos, ¿Cómo permite sancionar el Código Orgánico Integral Penal?
5. El derecho a la intimidad es afectado por el delito de apropiación fraudulenta de medios electrónicos, como ente sancionador, ¿Cómo actúa el sistema penal ecuatoriano al momento de reparación integral a la víctima?
6. ¿Cómo define a la seguridad informática?
7. Defina confidencialidad, integridad y disponibilidad sobre la apropiación fraudulenta de medios electrónicos.
8. Dentro de la gran cantidad de formas de cometer fraude en Internet, ¿Cuáles han sido las de mayor atribución para su juzgamiento?