UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIVERSIDAD CATÓLICA DE CUENCA

UNIDAD ACADÉMICA DE CIENCIAS SOCIALES.

CARRERA DE DERECHO.

TÍTULO:

ANÁLISIS JURÍDICO DEL CATFISHING EN TRANSACCIONES DE COMERCIO TELEMÁTICO EN ECUADOR: DESAFÍOS Y SOLUCIONES EN EL CONTEXTO DE LA SEGURIDAD CIBERNÉTICA.

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADA

AUTORA: KATERINE ALEXANDRA CORONEL RIVERA.

DIRECTORA: DRA. CARMEN ELIZABETH AREVALO VASQUEZ MGRT.

CUENCA – ECUADOR

2024

DIOS, PATRIA, CULTURA Y DESARROLLO

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE CIENCIAS SOCIALES.

CARRERA DE DERECHO.

TÍTULO:

ANÁLISIS JURÍDICO DEL CATFISHING EN TRANSACCIONES DE COMERCIO TELEMÁTICO EN ECUADOR: DESAFÍOS Y SOLUCIONES EN EL CONTEXTO DE LA SEGURIDAD CIBERNÉTICA.

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADA.

AUTORA: KATERINE ALEXANDRA CORONEL RIVERA.

DIRECTORA:DRA. CARMEN ELIZABETH AREVALO VASQUEZ MGRT.

CUENCA - ECUADOR

2024

DIOS, PATRIA, CULTURA Y DESARROLLO

Universidad Católica de Cuenca

DECLARATORIA DE AUTORÍA Y RESPONSABILIDAD

Declaratoria de Autoría y Responsabilidad

Katerine Alexandra Coronel Rivera portador(a) de la cédula de ciudadanía Nº **0106735400**. Declaro ser el autor de la obra: **Análisis Jurídico del Catfishing en Transacciones de Comercio Telemático en Ecuador: Desafíos y Soluciones en el Contexto de la Seguridad Cibernética**, sobre la cual me hago responsable sobre las opiniones, versiones e ideas expresadas. Declaro que la misma ha sido elaborada respetando los derechos de propiedad intelectual de terceros y eximo a la Universidad Católica de Cuenca sobre cualquier reclamación que pudiera existir al respecto. Declaro finalmente que mi obra ha sido realizada cumpliendo con todos los requisitos legales, éticos y bioéticos de investigación, que la misma no incumple con la normativa nacional e internacional en el área específica de investigación, sobre la que también me responsabilizo y eximo a la Universidad Católica de Cuenca de toda reclamación al respecto.

Cuenca, **29 de abril de 2021**

F: .....

Katerine Alexandra Coronel Rivera.

C.I. **0106735400**

Universidad Católica de Cuenca

CERTIFICO

Certifico que el presente Trabajo de Investigación fue desarrollado por KATERINE ALEXANDRA CORONEL RIVERA, con el Tema "ANÁLISIS JURÍDICO DEL CATFISHING EN TRANSACCIONES DE COMERCIO TELEMÁTICO EN ECUADOR: DESAFÍOS Y SOLUCIONES EN EL CONTEXTO DE LA SEGURIDAD CIBERNÉTICA", bajo mi supervisión.

Dra. CARMEN ELIZABETH AREVALO VASQUEZ.
Docente Tutora.

DEDICATORIA.

A mis padres Xavier Coronel y Verónica Rivera, su amor y apoyo han sido fundamentales en mi camino. Gracias a su sabiduría y esfuerzo, he aprendido a enfrentar los retos con valentía y determinación, a través de su ejemplo, he comprendido el valor del el trabajo duro, y que la constancia es clave para el éxito. Han sido guías esenciales en mi desarrollo académico y personal, inculcándome la importancia de la perseverancia. Les debo mucho de lo que soy y les agradezco de corazón.

A mi hermano José Coronel,ya que gracias al apoyo moral que me has brindado, me has demostrado que siempre hay una solución para cada situación. Tu optimismo y sabiduría son una guía invaluable en mi vida.

A mis queridos abuelos, Porfirio Coronel y Yolanda Piedra, cuyos consejos y buenos deseos han sido mi guía. Gracias a su sabiduría y amor, he logrado avanzar y crecer en la vida.

Mi prima Erika Coronel, por alentarme a siempre seguir adelante, aconsejarme y su apoyo incondicional.

A mi mejor amiga Michelle Urgiles, por siempre brindarme su amista y apoyo incondicional, alentándome a seguir adelante y cumplir con todos mis objetivos.

A mi querido perro Samuel, mi fiel compañero, cuya lealtad y compañía han sido un gran apoyo. Su incondicional amistad me ha motivado a seguir adelante.

Katerine Alexandra Coronel Rivera.

AGRADECIMIENTO

Agradezco a Dios por guiar mis pasos, y brindarme la fortaleza necesaria para alcanzar esta meta y proporcionarme la fuerza para enfrentar los desafíos que se han presentado en mi camino.

Agradezco a mis padres por su incondicional apoyo. Gracias a su esfuerzo, paciencia y dedicación, hoy tengo la fortuna de alcanzar una nueva meta en mi vida.

Mi más sincero agradecimiento a la Dra. Carmen Arévalo, cuya mentoría fue indispensable para la elaboración de este artículo. Su generosidad al compartir su sabiduría ha sido una guía esencial en mi investigación. Igualmente, extiendo mi gratitud al Ingeniero Marcel Villavicencio, por su dirección experta y los valiosos conocimientos impartidos, que han sido fundamentales para el desarrollo de este trabajo.

Katerine Alexandra Coronel Rivera

RESUMEN

En los últimos años Ecuador experimentó un crecimiento económico impulsado por la expansión de la conectividad a internet, el uso masivo de dispositivos móviles, la transformación digital y el impacto tecnológico de la pandemia por Covid-19. Este avance provocó un incremento en el número de tiendas virtuales, ofreciendo una amplia variedad de productos y servicios en la web, fortaleciendo la confianza de los consumidores en las compras en línea. Este progreso digital, también ha dado paso a nuevos tipos de delitos cibernéticos como el "Catfishing", término que hace referencia a la suplantación de identidades en los procesos del comercio telemático.

En esta investigación se realiza un análisis sobre el Catfishing en transacciones de comercio telemático en Ecuador, abordando detalladamente los desafíos y soluciones para reforzar la seguridad cibernética en este campo con miras en difundir sus efectos a la comunidad ecuatoriana sobre estos actos delictivos emergentes. El Catfishing constituye una práctica que implica suplantar identidades en línea con el fin de engañar a las personas y obtener ganancias económicas, este delito cibernético se convierte en una problemática real para la libre oferta-demanda que exige la comunidad globalizada. Por ello se resalta la importancia de comprender este fenómeno y concientizar los riesgos y consecuencias de estos ciberataques, para ello se estudiará el Catfishing y su impacto en el comercio telemático ecuatoriano a través del análisis de su normativa legal, con el fin de brindar una visión integral y critica sobre esta problemática.

Palabras-clave: *Suplantación de Identidad, Delitos Informáticos, Beneficios Económicos, Comercio Telemático, Seguridad Cibernética.*

ABSTRACT

In recent years, Ecuador has experienced economic growth due to increased Internet connectivity, widespread use of mobile devices, digital transformation, and the technological impact of the COVID-19 pandemic. This advancement has led to an increase in the number of virtual stores, offering a wide variety of online products and services and strengthening consumer trust in e-commerce. However, it has also led to new types of cybercrime, such as "catfishing," which refers to impersonation in e-commerce processes.

In this research, an analysis of catfishing in e-commerce transactions in Ecuador is conducted. The challenges and solutions are discussed to strengthen cybersecurity in this field and inform the Ecuadorian community about the effects of these emerging criminal acts. Catfishing is a practice that involves online impersonation to deceive people and obtain economic gains; this cybercrime becomes a real problem for the supply and demand required by the globalized community. Therefore, understanding this phenomenon and raising awareness of the risks and consequences of such cyber-attacks are crucial. For this purpose, catfishing and its impact on Ecuadorian e-commerce will be studied by analyzing its legal regulations to provide a comprehensive and critical view of this problem.

Keywords: *Identity Theft, Computer Crimes, Economic Benefits, E-Commerce, Cyber Security*

"Análisis Jurídico del Catfishing en Transacciones de Comercio Telemático en Ecuador: Desafíos y Soluciones en el Contexto de la Seguridad Cibernética."

"Legal Analysis of Catfishing in Telematic Commerce Transactions in Ecuador: Challenges and Solutions in the Context of Cybersecurity".

INTRODUCCIÓN

Con el auge de las tecnologías emergentes, la forma en que los seres humanos realizaban sus actividades cotidianas experimentó una transformación radical. Existe una transición de métodos manuales y presenciales a un entorno digital y virtual donde la confianza es crucial, especialmente dentro del Comercio Telemático. En este nuevo entorno, las transacciones electrónicas se fundamentan en la premisa de "pague primero, reciba después", lo que presenta desafíos y oportunidades únicos tanto para los consumidores como para las empresas.

La globalización virtual se convirtió en un pilar fundamental para las sociedades modernas, permitiendo un incremento significativo en la comunicación entre individuos y facilitando el intercambio de conocimientos. No obstante, esta nueva realidad también trajo consigo desafíos en cuanto a su control y regulación que ocasionaron el desarrollo de nuevos actos dolosos en estos espacios digitales, conocidos como delitos informáticos o ciberdelitos, que representan uno de los mayores peligros para la seguridad global en el siglo XXI (Arco Argudo, Pinos, & Mora, 2023).

Davara Rodríguez define al delito informático como: "la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevado a cabo utilizando un elemento informático y/o telemático o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software" (Davara Rodríguez, citado por Acurio Del Pino, 2016, p.10).

Esto quiere decir que los delitos informáticos son actividades ilegales que se llevan a cabo utilizando tecnología informática o telemática, específicamente mediante el uso de ordenadores, sistemas cloud (en la nube), plataformas de streaming, dispositivos móviles o internet. Estas actividades en la actualidad pueden abarcar una amplia gama de acciones, desde el acceso no autorizado a sistemas informáticos, la manipulación de datos

y el robo de información, hasta la difusión de virus informáticos o la ejecución de fraudes en línea.

Es así que, como consecuencia del incremento de los delitos informáticos, surgió el Catfishing, una práctica delictiva que se ha infiltrado en los sistemas de comercio telemático. Este nuevo ciberdelito es más complejo y difícil de identificar debido a su forma de operar lo que plantea retos adicionales para su prevención y erradicación. La falta de conocimiento y educación sobre el Catfishing por parte de los ciudadanos ecuatorianos contribuyó a su expansión, resaltando la importancia de fortalecer y mejorar la educación en seguridad digital, así como implementar medidas efectivas para proteger a los usuarios dentro de los sistemas económicos digitales.

Este estudio tiene como meta exponer este nuevo delito informático y la falta de adecuación del marco legal ecuatoriano frente a los nuevos ciberdelitos, además de contribuir al desarrollo de estrategias y medidas de seguridad que garantice la protección de los comerciantes telemáticos y sus clientes, promoviendo así un entorno seguro para la actividad comercial digital en el país.

METODOLOGIA

La metodología que se va a utilizar para el análisis de los capítulos de este artículo se centra en dos enfoques:

- Método analítico: los tres primeros capítulos se abordarán mediante el método analítico. Este enfoque iniciará con una exploración detallada de la naturaleza del delito informático, el fenómeno del Catfishing, la gestión del comercio telemático y las regulaciones correspondientes en Ecuador, incluyendo una comparativa con la legislación española. El análisis buscará determinar el impacto que ha generado este nuevo acto delictivo dentro del comercio telemático ecuatoriano, examinando conceptos, causas y diversas interpretaciones para sintetizar una comprensión global del tema.
- Método sintético: En el cuarto y último capítulo, se utilizará el método sintético, para orientar e integrar los elementos previamente analizados con el fin de reconstruir una visión completa del tema. El objetivo será analizar la posible incorporación del Catfishing al marco legal ecuatoriano y desarrollar soluciones que beneficien a la comunidad.

DESARROLLO

Determinar las generalidades del Catfishing en las transacciones de comercio telemático.

Los primeros delitos informáticos se remontan a las décadas de los 60 y 70, teniendo como objetivo principal interferir con los sistemas telefónicos o acceder a datos personales en computadoras. Durante este periodo, tales actos no eran considerados delitos graves debido a la limitada tecnología de la época y al hecho de que no causaban daños significativos a las víctimas más allá de asustarlas. No obstante, en la década de 1980, estos delitos informáticos se diversificaron y evolucionaron, pasando de acosar o asustar a las personas a prácticas como el espionaje, fraude, sabotaje, suplantación de identidades y la piratería, explotando las vulnerabilidades de los sistemas informáticos y aprovechándose de la falta de regulación estatal (Sain, s.f).

Esta situación impulsó a la Organización para la Cooperación Económica (OCDE) a iniciar un estudio en 1983 en París. Su objetivo era implementar normativas penales en la comunidad internacional que combatieran el uso indebido de los programas de computación. Es así que la OCDE definió al delito informático como "cualquier conducta ilegal, no ética o no autorizada que involucra el procesamiento automático de datos y/o la transmisión de datos" (Pablo A Palazzi, 2000, p.37, citado por, Quintero, s.f, p.3).

La llegada del internet y la World Wide Web en la década de los 90 y 2000 marcó un punto de inflexión en la nueva era digital, los delitos informáticos se multiplicaron y diversificaron dando lugar a prácticas como el hacking, phishing, grooming, ransomware, entre otros términos asociados a los delitos cibernéticos. Esta expansión de actividades ilegales en línea se debió al aumento de la conectividad global y la creciente dependencia de la tecnología digital (Acurio Del Pino, 2015).

En la actualidad, los sistemas informáticos han creado un ambiente propicio para la ejecución de delitos, conocido como entorno criminógeno, su función es facilitar el acceso a través de diferentes plataformas digitales para cometer una amplia gama de infracciones. A diferencia de los delitos tradicionales, los delitos informáticos carecen de límites físicos lo que les permite tener un mayor impacto en el espacio virtual. Además, en este entorno se almacena una gran cantidad de datos personales y financieros, lo que aumenta el riesgo de que estos sean interceptados o manipulados por personas inescrupulosas (Acurio Del Pino, 2015).

Como consecuencia, se ha incrementado la proliferación de los delitos informáticos y, debido a la conectividad global, los ciberdelincuentes pueden operar desde cualquier lugar del mundo con solo tener acceso a la red. De igual forma, la falta de conocimiento en seguridad informática contribuye a que las personas sean más vulnerables a estos ataques. Según el profesor Rovira Del Canto (2002, citado por Acurio Del Pino, 2015) existen tres factores que permiten esta proliferación:

- Desconocimiento de los nuevos sistemas de tratamiento de información.

Los usuarios no poseen conocimientos relacionados al uso de sistemas informáticos lo que incrementa el riesgo de ser víctimas de actos dolosos gracias a la masificación del uso del internet. Esta situación exige la creación de sistemas de seguridad para proteger la información personal y evitar pérdidas económicas, sanciones legales y daños a la reputación.

- La inexistencia y precariedad de los sistemas de seguridad.

Los sistemas de seguridad tradicionales no son suficientes para proteger la información en la era digital. Es necesario actualizar de forma constante los sistemas de seguridad y desarrollar nuevos modelos para estar a la vanguardia de la delincuencia informática.

- La falta de leyes normativas especiales.

En el pasado, las leyes tradicionales no eran suficientes para abarcar la complejidad de los delitos informáticos, por lo tanto, es necesario crear leyes que definan y sancionen de manera adecuada a los ciberdelitos. Estas leyes deberían incluir:

- La definición clara de los delitos informáticos.
- Establecer penas proporcionadas a la gravedad del delito.
- Facilitar la investigación y el enjuiciamiento de los delitos informáticos.
- Promover la cooperación internacional en la lucha contra la delincuencia informática (págs. 49-50).

El creciente desarrollo del entorno virtual, así como la falta de conocimiento en lo referente a seguridad digital, tienen como efecto el surgimiento de Catfishing, una práctica delictiva que se ha ido infiltrando gradualmente en el espacio virtual. Aunque aún no está formalmente reconocida en los marcos legales, representa un desafío creciente para los sistemas tecnológicos, poniendo de evidencia la necesidad de implementar normas que aborden estas nuevas formas de ciberdelitos.

Origen y evolución del Catfishing.

Catfishing deriva del inglés catfish que significa “pez gato”, este término se popularizó tras el lanzamiento del documental “Catfish” en 2010 donde su productor y protagonista, Nev Schulman, narra su experiencia con el Catfishing al establecer una relación sentimental con alguien a través de Internet, para posteriormente descubrir que la persona detrás de la pantalla no era quien decía ser.

Este documental no sólo expuso su experiencia personal, sino que también dio luz a un fenómeno que ocurre con frecuencia en el mundo digital. La relevancia del documental llevó a Schulman a crear y producir la serie “Catfish: mentiras en la red” para la productora MTV, en este programa se investigan casos reales de personas que han sido

víctimas de Catfishing, proporcionando así una mayor conciencia, comprensión y visibilidad sobre esta práctica engañosa (Kottemann, 2015).

El Catfishing, también conocido como suplantación de identidad, es un delito que implica el robo y uso de la identidad de una persona, empresa o compañía, para engañar en redes sociales o plataformas web. A diferencia de otros delitos informáticos como el hacking, phishing o grooming, el Catfishing se distingue por captar la identidad de una persona natural o jurídica de forma tan precisa que es difícil reconocer los perfiles falsos. Los delincuentes utilizan información personal, imágenes, vídeos, animaciones y todo contenido multimedia de otras personas para crear perfiles idénticos a los originales y su técnica de copiado es tan minuciosa y precisa que a simple vista las víctimas no suelen percibir el acto delictivo. Su objetivo, como se indicó anteriormente, es engañar a los usuarios con la premisa de obtener beneficios personales, económicos e incluso políticos, aprovechándose de los factores criminógenos de los delitos informáticos antes descritos. Esta práctica ha evolucionado hasta convertirse en una forma de ciberacoso, representando una preocupante patología social en el espacio virtual, afectando a individuos y organizaciones sin distinción alguna, causando incluso repercusiones en la propiedad intelectual y la seguridad en línea (Maheen, Ghani, & Syed, 2023).

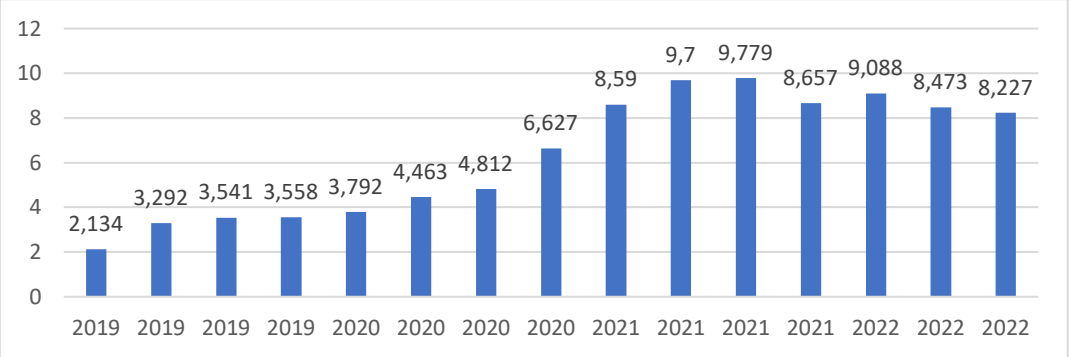
El ascenso del Catfishing dentro de la redes sociales y páginas de citas en Estados Unidos.

El Catfishing, tras ganar notoriedad con el documental producido por Schulman, experimentó un crecimiento significativo en los últimos 5 años, esto se reveló en un estudio realizado por AllAboutCookies.org (2023), con datos del FBI y la FTC. La investigación indica que este acto delictivo ha sido identificado como una estafa en la era digital, costando a las víctimas en Estados Unidos más de $500 millones de dólares en

2021. El análisis de estos datos resalta un aumento alarmante en la frecuencia y el impacto del Catfishing en la sociedad. Se destaca:

- *Las tendencias del Catfishing a lo largo del tiempo en Estados Unidos, entre los años 2019 y 2022:*

Figura 1. Casos de Catfishing en Estados Unidos periodo 2019-2022



Fuente: AllAboutCookies.org (2023).

El gráfico muestra que, en el primer trimestre de 2019, la FTC recibió 2,134 informes de Catfishing. Esta cifra aumentó constantemente en cada trimestre hasta alcanzar un máximo de 9,779 informes en el tercer trimestre de 2021, lo que representa un incremento del 358% en tan solo dos años y medio. Desde 2019, el promedio de informes trimestrales ha aumentado de 3,131 en 2019 a 8,596 en 2022, lo que implica un aumento de más del 174%. Actualmente, se estima que existen aproximadamente 4 veces más informes de estafas de Catfishing en comparación con principios de 2019 (Koebert, 2023).

- *El impacto del Catfishing en diferentes grupos de edad, entre los años 2019 y 2022:*

En la Tabla 1 se puede apreciar que las personas de 60 a 69 años reportan menos casos de Catfishing entre 2019 y 2022, pero son las que han experimentado mayores pérdidas económicas por este tipo de estafas, acumulando un total de 360 millones de dólares en cuatro años. Por otro lado, las personas de mediana edad (30-39 años) son las que reportan

más casos de Catfishing, aunque no son las más propensas a perder grandes sumas de dinero en estas trampas cibernéticas (Koebert, 2023)

Tabla 1. Casos de Catfishing por edad

Edad de la víctima	Casos totales	Total de dinero perdido	Cantidad promedio perdido por casos
20-29	17,479	$64,297,224	$3,679
30-39	18,598	$156,066,108	$8,392
40-49	17,876	$201,007,364	$11,245
50-59	17,331	$277,391,594	$16,006
60-69	15,426	$363,463,711	$23,562
70-79	6,898	$211,802,085	$30,705
80+	1,193	$36,324,476	$30,448

Fuente: AllAboutCookies.org (2023)

Análisis del Catfishing dentro del comercio telemático a nivel mundial.

El Catfishing fue inicialmente asociado con las redes sociales y las citas en línea, pero su alcance se extendió a los sistemas de comercio telemático aprovechándose de plataformas digitales. Es así que los ciberdelincuentes empezaron a usurpar la identidad de artistas y creadores de contenido, apropiándose indebidamente de obras de arte, música, fotografía y páginas web, lo que afecta la integridad y los derechos de autor.

El Catfishing puede manifestarse en diversas plataformas en línea como: Instagram, Twitter y Facebook. Está última red social cuenta con la plataforma de *Marketplace* que facilita la oferta y adquisición de bienes y servicios, lo que permite realizar transacciones desde cualquier lugar del mundo y ha sido la plataforma más afectada por el robo de las identidades de sus usuarios, se puede decir que el catfishing es el "Talón de Aquiles de Facebook". El Catfishing también se infiltró en aplicaciones de mensajería como WhatsApp, o incluso en sitios web dedicados a la promoción de contenido creativo como TikTok. Por estas razones es crucial que los usuarios de las plataformas digitales sean conscientes de los riesgos y tomen medidas para proteger su información y contenido (Maheen, Ghani, & Syed, 2023).

La pandemia de COVID-19 provocó una transformación en el comercio global y es el momento en el que, por las medidas de confinamiento implementadas por los

gobiernos de cada país, el comercio telemático se convirtió en una solución vital para mantener activa la economía. A pesar de la resistencia inicial al uso de los sistemas digitales, la necesidad impulso su adopción, esta situación ocasionó que, tanto grandes como pequeñas empresas, digitalicen sus operaciones y desarrollen plataformas en línea para comercializar sus productos y servicios. Este cambio no solo permitió la continuidad de sus actividades, sino que también generó nuevas oportunidades de mercado.

La acogida del comercio digital contribuyó para que la iniciativa "The eTrade for all (2021)" (Comercio Electrónico para todos) emitida en la Conferencia Ministerial de la UNCTAD en Nairobi, Kenia en el año 2016, gane relevancia en el año 2020. Este proyecto tiene como objetivo abordar las lagunas de conocimiento sobre el comercio telemático, desempeñando un papel importante en la sensibilización sobre oportunidades y riesgos dentro de este nuevo sistema económico; dando una visión más realista de los desafíos que enfrentan las empresas y comercios (United Nations, 2021).

Esta iniciativa permitió la integración global de países desarrollados y en vías de desarrollo a los nuevos sistemas económicos internacionales, abriendo un abanico de oportunidades para el crecimiento económico y la inclusión social. En el Gráfico 2 se puede observar los resultados de un estudio realizado por BlackSip que resalta el crecimiento y la adopción del comercio telemático en el año 2020 a nivel mundial.

Figura 2. Ventas en Retail Online en el mundo periodo 2016-2020

Fuente: BlackSip (2020)

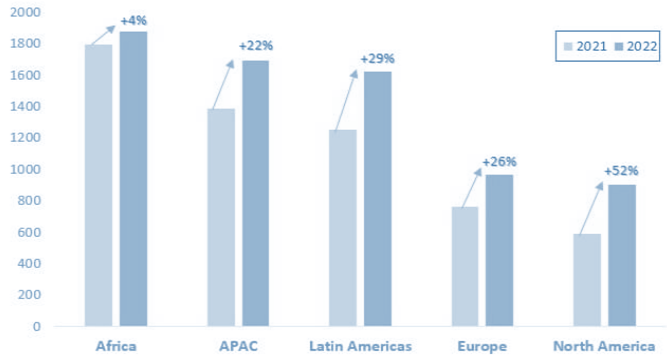
Los resultados señalan el incremento de las ventas globales en Retail Online, pasando de $1,84 billones de dólares en 2016 a $4,20 billones en 2020. Además, resalta

el crecimiento que ha tenido Latinoamérica, consolidando a la región como un actor clave en el mercado global de negocios digitales, no obstante, el desarrollo ha sido desigual, y Latinoamérica aún se encuentra por detrás de líderes como Asia-Pacífico, Norteamérica y Europa Occidental. (BlackSip, 2020).

Estudio del crecimiento de las amenazas cibernéticas en el mundo.

El crecimiento comercial conllevo avances tecnológicos y productivos, pero, también ha expuesto los problemas que enfrentan los países en contra de los ciberataques. Muchas naciones carecen de recursos económicos e infraestructura tecnológica para enfrentar los nuevos desafíos en delitos informáticos que surgieron a raíz del desarrollo de los sistemas económicos digitales. Un estudio realizado por Check Point Research recoge información relacionada a la tendencia de ciberataques en el año 2022, los datos están segmentados por volumen global, industria y geografía.

Figura 3. Promedio semanal de ciberataques por región 2021-2022



Fuente: Check Point (2023).

El Gráfico 3 indica que en 2022 se observó un aumento alarmante del 38% en los ciberataques a nivel global, impactando de manera principal a sectores críticos como la educación, el gobierno y la salud. América Latina, en particular, experimentó un incremento del 29% en estos ataques, lo que subraya la necesidad de fortalecer las medidas de seguridad digital en la región (Check Point, 2023).

Modos operandi del Catfishing dentro de las citas en línea y el comercio telemático.

Los catfishers empezaron a operar dentro de las plataformas para citas en línea creando perfiles utilizando la identidad de otras personas para atraer a sus víctimas. Primero establecían relaciones y tras ganar su confianza, solicitaban “favores” como él envió de material intimo (fotos y videos) o dinero. Una vez obtenido lo que querían, los catfishers desaparecían sin dejar rastro.

En el comercio telemático, los catfishers simulan ser comerciantes legítimos, creando perfiles con identidades robadas dentro de las redes sociales o páginas web que imitan a las auténticas, utilizando información completa como direcciones, imágenes, reseñas de supuestos clientes y números telefónicos falsos. Estos sitios presentan productos atractivos desde tecnología hasta artículos para el hogar, la variedad de productos que pueden llegar a presentar no tiene límites ya que su intención es llamar la atención de sus víctimas promocionándolos con publicidad engañosa en redes sociales. Cuando una persona muestra interés, el delincuente inicia un proceso para ganarse su confianza, informándole sobre sus promociones, descuentos y enviando fotografías falsas de los productos. Si la victima decide realizar la compra, se le pide que deposite el dinero por adelantado, una vez recibido el pago, el estafador transfiere rápidamente el dinero a otra cuenta, eliminando cualquier rastro del fraude y desapareciendo junto con la página web.

Estudio de la legislación ecuatoriana frente a los delitos informáticos, en el comercio telemático.

Ecuador al igual que otros países latinoamericanos, enfrenta desafíos en el desarrollo de la ciberseguridad. Aunque ha reconocido ciertos delitos dentro de sus códigos normativos, su legislación aún es limitada y tiende a abordar estos conflictos de manera superficial, sin atacar la raíz del problema (Ortiz Campos, 2019).

Es importante que la ley reconozca a los delitos para poder penalizarlos, ya que no se puede sancionar una conducta sin que esté explícitamente tipificada o reconocida dentro de un marco legal, lo que significa que las nuevas amenazas tecnológicas, como el Catfishing, requieren de la creación de tipos penales específicos. La estructura de un delito informático al igual que cualquier otro acto delictivo, se basa en tres pilares fundamentales: la tipicidad, la antijuricidad y la culpabilidad. Estas deben ofrecer garantías jurídicas y asegurar que solo se sancionen las conductas descritas en la ley.

En este caso, se resalta la tipificación de un delito como el elemento central para establecer un marco penal claro y eficaz. Para que un acto sea tipificado se deben identificar tres puntos claves que incluyen: la identificación del autor del delito, el medio utilizado para cometer el delito (sistemas informáticos) y el bien jurídico protegido (como puede ser la vulneración de derechos, o del patrimonio económico), es por ello que para que exista un debido control y percecusion de delitos como el catfishing primero se los debe tipificar o reconocer dentro de los códigos normativos (Zambrano, Dueñas Zambrano, & Macías Ordoñez).

Para este estudio se analizará la normativa vigente sobre los delitos informáticos reconocidos en el Ecuador, para ello se seguirá el orden jerárquico establecido en el artículo 425 de la Constitución ecuatoriana.

Constitución.

La Constitución de la República del Ecuador no menciona específicamente los delitos informáticos, pero, reconoce ciertos derechos que se relacionan con conductas cibernéticas como:

- El artículo 16.2 reconoce el derecho al acceso a las tecnologías de la información y comunicación, exigiendo al Estado protegerlo, eliminar las barreras de acceso y promover su servicio (Constitución de la República del Ecuador., 2008).
- Art 66: Se reconoce y garantiza a las personas: El derecho a la intimidad personal y familiar (Constitución de la República del Ecuador., 2008).
- El artículo 387 establece que el estado tiene la obligación de impulsar la generación y producción de conocimientos, así como fomentar la investigación científica y tecnológica (Constitución de la República del Ecuador, 2008).

Los artículos revisados ponen de evidencia que el reconocimiento de derechos es necesario, pero no suficiente para su protección efectiva en el ciberespacio. Esta situación revela una brecha normativa que pone en riesgo diversos principios constitucionales. Los principios constitucionales vulnerados se pueden apreciar a continuación en la Tabla 2.

Tabla 2. Principios constitucionales vulnerados

Principio.	**Descripción.**
Seguridad jurídica	El artículo 82 de la Constitución del Ecuador reconoce la seguridad jurídica como un derecho esencial, fundamentado en la coherencia entre las leyes y las acciones del gobierno con los principios y derechos establecidos en la Constitución. La seguridad jurídica demanda normativas claras y accesibles, así como su aplicación equitativa y objetiva por parte de las autoridades.
Tutela judicial efectiva	El artículo 75 de la Constitución garantiza el derecho a un acceso oportuno y efectivo a la justicia. Sin embargo, la falta de tipificación y reconocimiento de los delitos informáticos limita la capacidad de las víctimas para buscar reparación y protección ante la ley, ya que no hay un marco legal específico que respalde sus reclamos. Esto vulnera la garantía de que las personas

	puedan ejercer sus derechos y obtener una protección adecuada por parte del Estado en casos de delitos informáticos.
Principio de legalidad	El principio de legalidad establece que solo se puede castigar conductas previamente definidas por la ley. La falta de reconocimiento de delitos cibernéticos, como el "Catfishing", implica que no existe una base legal para sancionar estas acciones, lo que va en contra de este principio. Es necesario que las leyes se actualicen para abarcar nuevas formas de delitos surgidas con los avances tecnológicos, asegurando que todas las conductas delictivas estén debidamente contempladas en el marco legal.

Fuente: (Constitución de la República del Ecuador., 2008)

Tratados Internacionales.

Los Tratados Internacionales juegan un papel crucial en la regulación de la ciberdelincuencia a nivel global. Entre ellos se encuentra El Convenio de Budapest sobre la ciberdelincuencia, desarrollado por el Consejo de Europa en 2001, el cual es considerado la norma internacional más completa en la materia. Proporciona un marco legal eficaz en contra de las conductas ilícitas en línea y constituye una herramienta de derecho procesal para futuras investigaciones. Además, busca incentivar a los países miembros a participar en la cooperación internacional (Consejo de Europa, 2021).

A pesar que el Convenio de Budapest sobre la ciberdelincuencia ofrece un modelo efectivo para el desarrollo de las leyes ecuatorianas, el país aún no se adhiere a este tratado. La Asociación Ecuatoriana de Ciberseguridad (AECI) inclusive solicitó al gobierno que acepte unirse al Convenio, destacando la importancia de contar con una política penal común y mejorar la cooperación internacional para enfrentar los delitos informáticos. Sin embargo, el país no ha emitido respuesta alguna y esta falta de adhesión al tratado, coloca a Ecuador en una posición de desventaja en comparación con otros países Sudamericanos. Esta situación representa una barrera para llevar a cabo investigaciones efectivas y enfrentar la ciberdelincuencia de manera eficaz (Ortiz Campos, 2019).

Aunque Ecuador no aceptó formar parte de este Convenio, si llegó a aliarse con otros tratados internacionales, que, si bien no cuentan con el alcance normativo que brinda el Convenio de Budapest, si contribuyen a la protección contra aspectos específicos de la ciberdelincuencia o relacionados a su ejecución. Estos convenios internacionales son:

- Convenio de París: adoptado en 1883 regula la propiedad industrial incluyendo patentes, marcas y la represión de la competencia desleal, lo cual es crucial para la protección de la propiedad intelectual en el espacio digital (OMPI, s.f.)
- Convenio Internacional de Telecomunicaciones de Nairobi: este convenio firmado en 1982, establece principios y normas para la Cooperación Internacional en el ámbito de las telecomunicaciones y la seguridad cibernética (OMPI, s.f.).
- Convenio de Berna: ratificado por Ecuador en 1991, brinda protección a las obras literarias y artísticas ofreciendo a los creadores los medios para controlar el uso de sus obras y estableciendo un sistema de igualdad de tratas entre países miembros (OMPI, s.f.).
- Convenio de fonogramas: Rectificado en 1974, esta convención protege a los productores de fonogramas contra la reproducción no autorizada de sus grabaciones.

Código Orgánico Integral Penal.

El Código Orgánico Integral Penal (COIP) entró en vigencia en año 2014 y marcó un importante avance por la incorporación de nuevas figuras delictivas. Destaca la regulación y tratamiento de los delitos informáticos en el país ya que tipificó nuevos actos delictivos y amplió el alcance de las infracciones informáticas contempladas en el anterior código penal. El COIP enmarca a los delitos informáticos en la Sección Tercera titulada “Delitos contra la seguridad de los activos de los sistemas de información y

comunicación". Junto con otros artículos que se encuentran en el mismo código se intenta reforzar la protección legal frente a las amenazas digitales (Ortiz Campos, 2019). La Tabla 3 indica que el Código Orgánico Integral Penal en su esfuerzo por abordar la criminalidad en el ámbito digital, reconoció una serie de delitos informáticos, lamentablemente el progreso tecnológico acelerado, así como las prácticas en línea, dieron lugar a nuevos tipos de ciberdelitos que desafían las definiciones y categorías existentes.

Tabla 3. Tipicidad Del Delito Informático En El Código Orgánico Integral Penal Del Ecuador

Articulo	**Delito**	**Sentencia**
103.	Pornografía infantil	13-17
173.	Gromming	3-5
190.	Apropiación fraudulenta por medios electrónicos.	1-3
191.	Reprogramación o modificación de información de equipos terminales móviles.	1-3
192.	Intercambio, comercialización o compra de información de equipos terminales móviles.	1-3
193.	Remplazo de identificación de terminales móviles.	1-3
194.	Comercialización de terminales móviles.	1-3
211.	Supresión, alteración o suposición de la identidad y estado civil. - La persona que ilegalmente impida, altere, añada o suprima la inscripción de los datos de identidad suyos o de otra persona en programas informáticos.	1-3
229.	Revelación ilegal de base de datos.	1.3
230-186	Recolección (Pharming) y pesca (Phishing).	3-5
231.	Transferencia electrónica de activo patrimonial. (fraude informático)	3-5
232.	Ataque a la integridad de sistemas informáticos.	3-5
233.	Delitos contra la información pública reservada legalmente.	3-5
234.	Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.	3-5

Fuente: (Ramirez, 2017).

Entre estos nuevos delitos se encuentra el Catfishing o suplantación de identidad en línea, este delito aún no es tipificado de forma correcta dentro del marco legal actual del COIP, sumado a esto, el Catfishing representa un foco de numerosas denuncias en

Ecuador desde el año 2014. Sobre ello, un estudio realizado por la Fiscalía General del Estado recoge los siguientes datos expuestos en la Tabla 4.

Tabla 4.Número de denuncias sobre delitos informáticos en Ecuador

Tipos de delito	**2014**	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**Total**
Suplantación de identidad.	1335	3920	4152	3676	4180	4607	2162	24052
Falsificación y uso de documentos falsos.	1048	2594	3117	3183	3292	3231	1448	17913
Apropiación fraudulenta por medios electrónicos.	507	1280	1045	960	1451	1746	1033	8022
Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.	54	141	145	218	236	246	175	1215
Contacto con la finalidad sexual con menores de dieciocho años por medios electrónicos.	21	80	108	159	202	166	85	821
Ataque a la integridad de sistemas informáticos.	49	77	76	86	87	113	51	539
Intercepción ilegal de datos.	38	55	82	63	41	87	45	411
Transferencia electrónica de activo patrimonial.	17	59	47	54	38	49	31	295
Revelación ilegal de datos.	29	24	24	22	44	34	18	195
Total, por año.	3118	8230	8796	8421	9571	10279	5048	53463

Fuente: (El Universo, 2020)

El estudio muestra que en Ecuador desde el año 2017, antes de la pandemia del Covid-19, se registraron 8,421casos de denuncias por delitos informáticos, esta cifra ascendió a 9,571 en 2018 y a 10,279 en 2019, demostrando una tendencia ascendente que continúa hasta hoy. En esta categoría de crímenes, la suplantación de identidad a través de medios electrónicos representa el delito cometido con mayor frecuencia (El Universo, 2020).

Catfishing y el delito de suplantación de identidad.

Como ya se mencionó anteriormente, el catfishing es una forma de suplantación de identidad digital, y a diferencia de la suplantación de identidad tradicional que puede ocurrir cara a cara, el catfishing se desarrolla en el ciberespacio. El artículo 212 del

Código Orgánico Integral Penal establece penas para la suplantación de identidad, pero no especifica su aplicación en el contexto digital. El artículo no fue diseñado considerando la suplantación de identidad en línea, lo que puede llevar a interpretaciones erróneas de la ley y en consecuencia a una protección insuficiente para las víctimas de estos delitos modernos:

> Art 212.- Suplantación de identidad: la persona que de cualquier forma suplante la identidad de otra para obtener un beneficio para si o para un tercero, en perjuicio de una persona, será sancionada con pena privativa de libertad de uno a tres años. (Código Orgánico Integral Penal., 2014)

El catfishing y el delito de estafa.

El catfishing comparte ciertas características con el delito de estafa, pero posee particularidades que justifica su consideración como un delito independiente. El Artículo 186 del COIP define la estafa como un acto que busca un beneficio patrimonial a través del engaño, lo que implica una inducción al error que resulta en un perjuicio económico para la víctima o un tercero. Sin embargo, el catfishing va más allá de la mera afectación patrimonial, ya que implica la suplantación de una identidad en línea, con el potencial de dañar la confianza, la seguridad emocional y la reputación de las personas, comerciantes o compañías, así como de influir en el ámbito político y social mediante la desinformación y la manipulación.

El catfishing puede tener un impacto devastador en múltiples esferas, no solo económicas, sino también políticas y sociales. Económicamente, puede provocar la pérdida de fondos y dañar la reputación de empresas, afectando su valor y confianza en el mercado. Políticamente, la suplantación de identidades puede ser utilizada para influir en elecciones o desestabilizar instituciones. Socialmente, el catfishing erosiona la confianza en las interacciones en línea y puede causar daño psicológico a las víctimas.

Dada la complejidad y el alcance del catfishing, es crucial que se le dé un tratamiento legal más específico y efectivo. La tipificación del catfishing como un delito independiente permitiría una mayor protección a las víctimas, una persecución más efectiva y una prevención más adecuada. Además, al considerar el impacto del catfishing en áreas económicas, políticas y sociales, se hace evidente la necesidad de un tratamiento específico para este delito, que vaya más allá de ser simplemente una forma de estafa.

Bienes jurídicos vulnerados.

Todo delito ya sea tradicional o cibernético tiene como consecuencia la vulneración de un bien jurídico, este concepto se sustenta en un interés o valor protegido por la ley debido a su importancia para el individuo o la sociedad; cuando se comete un delito esté bien jurídico se ve afectado o amenazado. En el caso del catfishing existen dos bienes jurídicos que se ven afectados que son el derecho a la identidad y el patrimonio económico, esta particularidad es lo que lo diferencia del delito de suplantación de identidad y el delito de estafa que ya son reconocidos por el COIP:

La estafa y el catfishing son dos fenómenos que, aunque comparten ciertas similitudes, tienen diferencias fundamentales en sus objetivos y métodos. La estafa tradicionalmente se ha enfocado en el engaño para obtener beneficios económicos, aprovechándose de la confianza de las víctimas para despojarlas de sus bienes materiales. Por su parte, el catfishing es un tipo de estafa que se da específicamente en el ámbito digital. Los estafadores que practican el catfishing suelen poseer habilidades avanzadas en tecnología y son expertos en la manipulación social, lo que les permite robar identidades en internet y crear perfiles idénticos a los originales con gran credibilidad.

El catfishing no solo busca un beneficio económico, sino que también pone en riesgo la información personal de las víctimas. En este sentido, el catfishing representa una amenaza para un nuevo bien jurídico: la seguridad de nuestros datos digitales.

Mientras que la estafa se centra en proteger el patrimonio económico, el catfishing extiende su campo de acción para incluir la protección de la privacidad y la confianza en línea, además de los bienes materiales.

Es crucial reconocer que ambos delitos, estafa y catfishing, requieren atención y sanciones adecuadas para preservar la seguridad en el entorno digital. La estafa atenta contra nuestras posesiones materiales, mientras que el catfishing va más allá, comprometiendo nuestra privacidad y la integridad de nuestra identidad en el ciberespacio. La lucha contra estos delitos es fundamental para mantener la confianza en las interacciones digitales y asegurar que nuestra información personal permanezca protegida de actores malintencionados.

Ley De Comercio Electrónico, Firmas Y Mensajes De Datos

Una de las primeras iniciativas que tuvo Ecuador para proteger el espacio digital fue la promulgación de la Ley de Comercio Electrónico Firmas y Mensajes de Datos en abril de 2002, inspirada en la ley modelo emitida por la Comisión de las Naciones Unidas para el Derecho Mercantil CNUDMI, cuyo propósito es impulsar el comercio telemático a nivel mundial. La Ley de Comercio Electrónico Firma y Mensajes de Datos establece fundamentos esenciales, así como define derechos y responsabilidades para los actores del comercio digital, abarcando elementos como la firma electrónica y la gestión de mensajes de datos. Su influencia es notable en los derechos fundamentales de los ciudadanos ecuatorianos ya que incide en aspectos vitales como la privacidad, el debido proceso y los derechos del consumidor, así como la libertad empresarial contractual y de expresión (Acuario Del Pino, 2016).

En esta ley los delitos informáticos se abordan en el capítulo I del título V, comprendiendo los artículos 57 al 64. Su propósito es establecer una base normativa

sólida para el Código Orgánico Integral Penal, mejorando así la articulación y redacción de las normas que rigen los delitos informáticos (Sosa Meza, 2005).

Tabla 5. Delitos Informáticos Regulados Por La Ley De Comercio Electrónico, Firmas Y Mensajes De Datos.

Delitos Informáticos Regulados Por La Ley De Comercio Electrónico, Firmas Y Mensajes De Datos.	**Artículo**
Violación al derecho a la intimidad en documentos con soporte electrónico.	Art. 58 y 64.
Violación o divulgación de información secreta contenida en documentos con soporte electrónico.	Art. 58.
Obtención y utilización no autorizada de información.	Art. 58.
Destrucción o supresión de documentos con soporte electrónico por parte de personas que tuvieren su resguardo a cargo.	Art. 59.
Falsificación electrónica.	Art. 60.
Daños informáticos.	Art. 61.
Apropiación ilícita.	Art. 62.
Estafa utilizando medios electrónicos o telemáticos	Art. 63.

Fuente: Sosa Meza (2005)

La ley de Comercio Electrónico Firmas y Mensajes de Datos presentó un impacto significativo a nivel nacional por su influencia internacional, a pesar de ello, la aplicación de esta ley enfrenta desafíos por la falta de infraestructura tecnológica adecuada y el acceso limitado a equipos necesarios para su operación, lo que ha impedido su pleno funcionamiento. Además, existe el desconocimiento y falta de educación entre los ciudadanos ecuatorianos respecto a la ley, lo que dificulta su comprensión y aplicación efectiva.

Un claro ejemplo de esta problemática recae en el uso de firmas electrónicas, muchos ecuatorianos aún no saben cómo utilizarlas correctamente y la mayoría de las veces entregan sus claves y datos personales de acceso de este medio de firma digital a terceras personas, siendo en muchos casos engañados por los criminales que se roban sus firmas y suplantan su identidad. Estos incidentes exponen la necesidad de una mayor educación y recursos para asegurar el cumplimiento adecuado de la ley.

Ley Orgánica De Protección De Datos Personales.

El 19 de septiembre de 2019, Ecuador se vio afectado por una de las mayores filtraciones de datos de su historia. Cerca de 20,8 millones de registros, incluyendo información sensible de ciudadanos ecuatorianos, extranjeros e incluso fallecidos como nombres completos, números de cédula, direcciones, teléfonos, datos financieros e incluso historiales médicos fueron expuestos al mundo (Infinito Digital, 2019).

La respuesta inicial del Gobierno ecuatoriano fue negar la filtración, pero, la presión pública y la evidencia contundente los llevó a iniciar una investigación sobre el incidente. El estudio realizado por el Estado reveló que la empresa responsable de la filtración era Novaestrat, una empresa ecuatoriana de marketing y análisis; la información confidencial había sido almacenada en un servidor ubicado en Miami sin las medidas de seguridad adecuadas lo que facilitó el acceso no autorizado a los datos personales (BBC News Mundo, 2019).

Este incidente impulsó la creación la Ley Orgánica de Protección de Datos Personales (LOPDP) el 26 de mayo del año 2021, respaldada por entidades públicas y privadas. La ley se convirtió rápidamente en una norma jurídica fundamental para garantizar la protección de la información confidencial proporcionada por los usuarios a diversas instituciones; su objetivo es otorgar a los ciudadanos un mayor control sobre su información personales, promover la transparencia en el manejo de los datos por parte de las instituciones y sancionar el uso indebido de la información (Guerrón, 2021).

Además, esta ley fortalece la aplicación de los códigos existentes y se ajusta al Sistema de Gestión de Seguridad de la Información para alienarse con la norma ISO/IEC 27001, un estándar internacional que dicta los requisitos para sistemas tecnológicos más seguros implementando un proceso de 5 etapas: Implantación de políticas que aseguren la calidad y seguridad de los datos; Proyección del Sistema de Gestión; Control y análisis

de riesgos; Elaboración de normas; Control de aseguramiento mediante un modelo PHVA (Planificar-Hacer-Verificar-Actuar) (Cabezas Mena & Lucas Franco, 2023).

La Estrategia Nacional de Ciberseguridad del Ecuador.

En el año 2021, con la llegada del presidente Guillermo Lasso al poder, se establece La Estrategia Nacional de Ciberseguridad del Ecuador propuesta por Vianna Maino, Ministra de Telecomunicaciones y Sociedad de la Información. Consiste en un documento que establece políticas y acciones necesarias para garantizar la seguridad cibernética en el país. Esta estrategia tiene como objetivo proteger los sistemas de información y la infraestructura tecnológica de Ecuador frente a las amenazas digitales, abordando diversos aspectos relacionados con la ciberseguridad como: prevención y detección de incidentes, la protección de datos personales, la educación y conciencia e inseguridad cibernética, la Cooperación Internacional en materia de seguridad digital, entre otros (Ministerio de Telecomunicaciones y Sociedad de la Información, 2021).

A pesar de ello, la estrategia ha tenido que navegar por un entorno de limitaciones presupuestarias que restringieron su alcance y efectividad. La falta de infraestructura tecnológica adecuada y una normativa sólida representan obstáculos adicionales que impiden la realización de sus objetivos estratégicos. Estos factores resaltan la importancia de una inversión sostenida y el desarrollo de un marco legal para fortalecer la ciberseguridad nacional.

Análisis de la legislación española frente al fenómeno del Catfishing.

España tiene un impacto significativo en la regulación de los derechos digitales y la seguridad en línea en Ecuador, esta influencia se observa especialmente en áreas como la protección de datos y la seguridad en el comercio electrónico. Ecuador ha adoptado leyes alineadas con los principios de la normativa española como la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, para fortalecer la seguridad de la información y su intercambio electrónico.

En la normativa española los delitos informáticos, aunque no son clasificados en una categoría especial, están cubiertos por diversas normativas que incluyen el Código Penal, la LOPDGDD y la LSSI. Estas regulaciones abordan conductas ilícitas en línea, tales como delitos contra la intimidad, la imagen, el patrimonio, el orden socioeconómico y las falsedades documentales (Cuero, 2015). Dentro del contexto jurídico español, la respuesta legal a los delitos informáticos ha avanzado significativamente, de manera particular con la Ley Orgánica 1/2015 que reformó el Código Penal adaptándolo a las dinámicas del ciberespacio y la tecnología moderna.

La legislación de España continúa progresando para combatir de manera eficiente las nuevas modalidades de ciberdelincuencia, asegurando una protección efectiva en el espacio digital. Las sanciones por delitos informáticos en España se escalan según la seriedad del delito, pudiendo ir desde multas económicas hasta penas de prisión de varios años.

El Catfishing, aunque no este definido explícitamente en la ley española, se enfrenta a través del delito de suplantación de identidad en línea o usurpación del estado civil, penalizado en el artículo 401 del Código Penal. El artículo determina que la apropiación ilícita de la identidad de una persona con el objetivo de obtener un beneficio o provocar un daño, aunque este no se llegue a producir, será sancionado con una pena de

libertad de 6 meses a 3 años. pero este acto delictivo podrá ser sancionado siempre y cuando cumpla con los requisitos exigidos por la ley:

- Los actos deben ser duraderos para que causen confusión.
- La suplantación debe ser de una persona real, ya sea viva o fallecida.
- El objetivo de la suplantación de ser obtener un beneficio o causar daño.
- Deben ejercer derechos o acciones que correspondan a la víctima.

El simple hecho de hacerse pasar por otra persona no constituye un delito si es que no cumple con estos requisitos, aun cuando esta suplantación de identidad llegue a perjudicar a una persona. Esto lo afirma la sentencia de la Sección 6ª de la Audiencia Provincial de Madrid 322/2010 de 20 de julio (EDJ 2010/173334), donde establece que, para que se configure el delito de usurpación del estado civil, no es suficiente el robo momentáneo o parcial, si no que se requiere la continuidad y persistencia del delito, ejerciendo sus derechos y cumpliendo sus obligaciones dentro de su entorno familiar o social (González Sánchez, s.f.).

El Catfishing y su incorporación al marco legal ecuatoriano y soluciones.

La transformación tecnológica en Ecuador ha experimentado un notable impulso en los últimos años, especialmente debido a la adopción de plataformas en línea por parte de las empresas. Este cambio se aceleró con la crisis sanitaria del COVID-19, llevando a aproximadamente el 20% de los negocios ecuatorianos a establecer canales de venta en línea, ya sea mediante sus propios sitios web o a través de plataformas de terceros. En 2018, las ventas digitales en el país alcanzaron los 11.970 millones de dólares, reflejando el crecimiento del comercio electrónico. Ante este auge comercial, Ecuador ha realizado ajustes en su marco legal, reconociendo el derecho al acceso tecnológico en su Constitución y reformando códigos normativos para incorporar la realidad virtual.

Sin embargo, la rápida evolución tecnológica ha resultado en la obsolescencia de ciertos códigos legales, generando vacíos que dificultan la prevención y sanción de ciberdelitos. Un ejemplo de esto es el Catfishing, una modalidad de ciberdelincuencia que se beneficia de estos vacíos legales. Los catfishers recopilan información de manera fraudulenta en el entorno digital, usurpan la identidad de comerciantes y crean historias ficticias para vender productos. Engañan a los clientes para que realicen pagos anticipados y, tras recibir el dinero, desaparecen sin entregar lo prometido. Esta práctica subraya la necesidad de una clasificación detallada para su persecución, identificación y procesamiento efectivos. Es por ello que para abordar los desafíos del Catfishing y garantizar la seguridad en el comercio telemático es fundamental fomentar la educación y sensibilización sobre la seguridad cibernética entre los usuarios (ECUADORDOMAIN S.A., 2023).

Es fundamental incorporar normas que especifiquen, definan y castiguen el Catfishing teniendo en cuenta su naturaleza y las distintas maneras en que se presenta. Para combatir eficazmente a este delito informático se proponen las siguientes soluciones:

1. Reforma legislativa:

El Código Orgánico Integral Penal reconoce una amplia gama de delitos y los clasifica detalladamente. No obstante, la evolución tecnológica acelerada ha provocado que ciertas normativas se vuelvan obsoletas. Por ello, es imperativo actualizar el COIP para incluir delitos emergentes como el catfishing, especialmente en la era digital actual. El catfishing, que implica la suplantación de identidad en línea, tiene consecuencias severas tanto para individuos como para entidades comerciales. Este acto no solo vulnera la identidad personal de las víctimas, sino que también puede desencadenar efectos devastadores en su situación financiera. Los comerciantes en línea, por ejemplo, pueden experimentar daños considerables en su reputación y la confianza de sus clientes cuando son víctimas de usurpación de identidad. Esto puede resultar en una percepción negativa extendida y una desconfianza hacia la marca, lo que podría llevar a pérdidas económicas. Además, los clientes de estos comerciantes enfrentan riesgos significativos, ya que el catfishing amenaza su seguridad financiera; al intentar comprar productos en línea, pueden ser engañados para depositar dinero en cuentas fraudulentas.

El catfishing es un fenómeno que afecta tanto a la identidad personal como al patrimonio económico de las personas. Esta dualidad lo distingue de delitos como la estafa, que se centra en el engaño para obtener un beneficio económico, o la suplantación de identidad, que atenta contra el derecho a la identidad, pero no siempre tiene una motivación económica. La inclusión del catfishing en la Sección Décima del Código Orgánico Integral Penal, dedicada a los "Delitos contra el derecho a la identidad", sería apropiada porque esta sección ya contempla delitos que atentan contra la identidad personal. Además, podría adaptarse para abarcar las particularidades del catfishing, como el uso de medios digitales y la posible afectación económica (Código Orgánico Integral Penal.).

Reconocer el catfishing como un delito autónomo permitiría desarrollar medidas preventivas específicas y fortalecer la seguridad y transparencia del entorno comercial digital. La confianza y la autenticidad son esenciales en las relaciones de consumo; proteger legalmente contra prácticas engañosas como el catfishing consolidaría la integridad del mercado digital. Disponer de procedimientos legales claros para perseguir y sancionar estas conductas es vital para recuperar y mantener la confianza en el comercio electrónico y las interacciones online.

Por otro lado, la Sección de "Delitos contra la seguridad de los activos de los sistemas de información y comunicación" del COIP se enfoca en la protección de la infraestructura informática y la integridad de los datos, más que en la identidad personal o el patrimonio económico de individuos. Incorporar el catfishing en esta sección podría diluir su enfoque y restar efectividad a las medidas legales contra este tipo de delito. En cambio, al situarlo dentro de los delitos contra la identidad, se subraya la importancia de proteger la identidad personal en el ámbito digital y se proporciona un marco legal más coherente para abordar las consecuencias económicas del catfishing (Código Orgánico Integral Penal.).

2. Colaboración internacional.

La participación de Ecuador en el Convenio de Budapest sobre la Ciberdelincuencia representaría un avance crucial en la lucha contra los crímenes informáticos. Este tratado internacional, el primero de su tipo, busca armonizar las leyes nacionales en torno a la ciberdelincuencia, facilitar la cooperación legal entre países y mejorar las capacidades investigativas de las autoridades. Para Ecuador, esto podría traducirse en una mayor protección contra delitos como el fraude electrónico y la suplantación de identidad los cuales son cada vez más comunes en la era digital. Además, permitiría al país compartir y recibir información crítica sobre las tácticas y

procedimientos de los ciberdelincuentes, un elemento esencial para prevenir y responder a ataques futuros.

3. Capacitación y concientización.

La capacitación y concientización son fundamentales en la lucha contra el Catfishing dentro del comercio telemático, los programas educativos en seguridad cibernética en instituciones educativas y centros de trabajo pueden proporcionar las herramientas necesarias para identificar y evitar fraudes en línea. Estos programas deben incluir ejemplos prácticos de Catfishing destacando la importancia de verificar la identificación de las personas y empresas en el entorno digital.

Las campañas de concientización juegan un papel crucial puesto que conforman una oportunidad para elevar el conocimiento público sobre los peligros del Catfishing y otros delitos informáticos. Estas campañas pueden utilizar diversos medios de comunicación como redes sociales y publicidad en línea para difundir mensajes sobre las señales de alerta y las medidas preventivas.

Por último, la formación especializada del personal judicial es fundamental para que puedan seguir el ritmo de las tácticas de los estafadores y aplicar la ley de manera efectiva, esto incluye entender la naturaleza técnica del comercio telemático y las formas en que el Catfishing puede afectar tanto individuos como empresas.

CONCLUSIONES

El comercio telemático en Ecuador, como en muchas otras partes del mundo, ha experimentado un crecimiento exponencial, facilitando el intercambio de bienes y servicios a través de medios electrónicos. Sin embargo, este avance también ha traído consigo un aumento en los delitos cibernéticos, entre los cuales el catfishing se ha destacado por su impacto negativo tanto en individuos como en la seguridad económica del país. El catfishing, que implica la suplantación de la identidad en línea de una persona, comerciante o empresa, afecta no solo al patrimonio económico de las víctimas sino también a su derecho de identidad.

La importancia de tipificar el catfishing dentro del Código Orgánico Integral Penal como delito independiente no significa negar su relación con la estafa, pues la intención es reconocer las particularidades de este tipo de engaño y las graves consecuencias que puede tener para las víctimas. A diferencia de los delitos tradicionales de estafa o suplantación de identidad, el catfishing se caracteriza por la vulneración dual de bienes jurídicos: el derecho de identidad y el patrimonio económico. Esta dualidad hace que el catfishing sea particularmente dañino y, por lo tanto, requiere un enfoque legal distinto para su tratamiento y sanción.

La Sección Décima del COIP, dedicada a los "Delitos contra el derecho a la identidad", proporciona un marco legal que podría adaptarse para abordar el catfishing de manera más directa. Esta sección protege aspectos fundamentales de la identidad personal, que son precisamente los que se ven comprometidos en los casos de catfishing. Al tipificar el catfishing como un delito independiente, se facilitaría la aplicación de medidas legales adecuadas, permitiendo una persecución más efectiva de los infractores y una mejor protección para las víctimas.

Además, la tipificación independiente del catfishing en el COIP permitiría la creación de políticas públicas y estrategias de prevención más enfocadas, educando a la población sobre los riesgos asociados con las interacciones en línea y cómo protegerse de posibles engaños. También promovería una mayor conciencia sobre la gravedad de estos delitos y la importancia de respetar la identidad y el patrimonio de los demás en el espacio digital.

REFERENCIAS BIBLIOGRÁFICAS

Acurio Del Pino, S. (2015). Derecho Penal Informático. Corporación de Estudios y Publicaciones (CEP). Obtenido de file:///C:/Users/Usuario/Downloads/Derecho_Penal_Informatico%20(1).pdf

Acuario Del Pino, S. (2016). *Delitos Informáticos: Generalidades.* Obtenido de Delitos Informáticos: Generalidades: https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Arco Argudo, M., Pinos, K. M., & Mora, M. F. (2023). Análisis comparativo de la Ley Orgánica de Protección de Datos Personales del Ecuador con la legislación colombiana desde un enfoque de ciberseguridad y delitos informáticos. *Revista Ibérica de Sistemas e Tecnologias de Informação*, 100-114. Obtenido de https://www.proquest.com/docview/2865402056/fulltextPDF/970FEC246FD24024PQ/1?accountid=61870&sourcetype=Scholarly%20Journals

Asamblea Nacional del Ecuador. (2008). *Constitución de la República del Ecuador.* Quito, ECUADOR. Obtenido de https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador_act_ene-2021.pdf

ASAMBLEA NACIONAL DEL ECUADOR. (10 de febrero de 2014). Código Orgánico Integral Penal. *Código Orgánico Integral Penal.* Ecuador. Obtenido de file:///C:/Users/Usuario/Downloads/CompletosSinConcordanciaspdf1070225_-_C%C3%83_DIGO_ORG%C3%83_NICO_INTEGRAL_PENAL__-_COIP.pdf

BBC News Mundo. (16 de septiembre de 2019). *Filtración de datos en Ecuador: la "grave falla informática" que expuso la información personal de casi toda la población del país sudamericano*. Obtenido de BBC News Mundo: https://www.bbc.com/mundo/noticias-america-latina-49721456

BlackSip. (2020). *Reporte de Industria: El e-commerce en Ecuador 2020.* https://content.blacksip.com/hubfs/Reporte%20industria%202020%20Ecuador_V2%20(2)%20(1).pdf?utm_campaign=ReporteIndustria_20_EC&utm_medium=email&_hsmi=116793699&_hsenc=p2ANqtz--pAGY4eBinFEhDJ0zO-E8MWy4teisC2elAOtpzowL2mwMq1lYtWnUkC-d0ja1ykEUPdNJfE_vE3nehvk: VTEX- DIGITAL COMMERCE PARTNERS.

Cabezas Mena, D. F., & Lucas Franco, G. S. (2023). *Análisis comparativo de la Ley Orgánica de Protección de Datos Personales del Ecuador con la Legislación Española desde un enfoque de ciberseguridad y delitos informáticos.* Proyecto de titulación con componentes de investigación aplicada y/o de desarrollo., Universidad Politécnica del Ecuador-Cuenca, Cuenca. Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/25114/1/UPS-CT010600.pdf

Check Point. (5 de enero de 2023). *Check Point Research informa de un aumento del 38% en los ciberataques globales de 2022*. Obtenido de checkpoint.com: https://blog.checkpoint.com/2023/01/05/38-increase-in-2022-global-cyberattacks/#:~:text=Global%20cyberattacks%20increased%20by%2038,%2Dlearning%20post%20COVID%2D19

Consejo de Europa. (2021). *El Convenio de Budapest sobre la Ciberdelincuencia.* Council of Europe. Francia: División de Ciberdelito. DGI. Obtenido de https://rm.coe.int/cyber-buda-benefits-junio2021a-es/1680a2e4de

Cuero, J. (22 de junio de 2015). *Codigo Penal Español*. Obtenido de Informática Jurídica > Código > Código Penal Español: https://www.informatica-juridica.com/codigo/codigo-penal-espanol/

ECUADORDOMAIN S.A. (2023). *Comercio Electrónico en Ecuador 2023: Impulso y Oportunidades.* NIC.ec-Beta. Obtenido de

https://revistaidentidad.ec/2023/05/16/comercio-electronico-ecuador-2023-impulso-oportunidades/

El Universo. (27 de septiembre de 2020). Los delitos informáticos crecen en Ecuador; cada clic en la web deja su rastro. *El Universo*. Obtenido de https://www.eluniverso.com/noticias/2020/09/27/nota/7991905/delitos-informaticos-internet-casos-reales-redes-sociales-ecuador/

González Sánchez, P. (s.f.). *Delito de usurpación de Estado Civil.* Obtenido de ABOGADOS PENALISTAS EN MADRID: https://www.pgsabogadospenalistas.com/blog/delito-usurpacion-estado-civil/

Guerrón, J. (2021). *Ecuador y su primera Ley Orgánica de Protección de Datos Personales.* Obtenido de AEC GOVERTIS: Asociación Española para la Calidad: https://dpd.aec.es/ecuador-y-su-primera-ley-organica-de-proteccion-de-datos-personales/

Infinito Digital. (16 de septiembre de 2019). *La filtraciòn de datos en boca de todos*. Obtenido de Infinito Digital-Carrera de Comunicación | UPS-Q: http://indi.ups.edu.ec/en-boca-de-todos-con-la-filtracion-dedatos-2

Koebert, J. (24 de Agosto de 2023). Catfish Capitals: These Are the Places You're Most Likely To Fall Victim to a Catfishing Scam. (C. McNally, Ed.) *All About Cookies*. Obtenido de All About Cookies: https://allaboutcookies.org/catfishing-scams-by-state

Kottemann, K. L. (2015). *ProQuest.* (P. LLC, Ed.) Obtenido de ProQuest: file:///C:/Users/Usuario/OneDrive/Escritorio/TITULACION/CATFISHING%201%20(1).pdf

Maheen, S., Ghani, A., & Syed, A. (21 de Marzo de 2023). Facebook as a Tool of Catfishing: An Analytical Study of University Students. *Human Nature Journal*

of Social Sciences, 464-469. Obtenido de Facebook como herramienta de catfishing: un estudio analítico de estudiantes universitarios: file:///C:/Users/Usuario/OneDrive/Escritorio/TITULACION/37-360-Research+Article+(Final+Copy).pdf

Maheen, S., Ghani, A., & Syed, A. (21 de Marzo de 2023). Facebook as a Tool of Catfishing: An Analytical Study of University Students. *Human Nature Journal of Social Sciences*, 464-469. Obtenido de Facebook como herramienta de catfishing: un estudio analítico de estudiantes universitarios: file:///C:/Users/Usuario/OneDrive/Escritorio/TITULACION/37-360-Research+Article+(Final+Copy).pdf

Ministerio de Telecomunicaciones y Sociedad de la Información. (2021). ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DEL ECUADOR-Vianna Maino. *ESTRATEGIA NACIONAL DE CIBERSEGURIDAD DEL ECUADOR-Vianna Maino*. ECUADOR. Obtenido de https://asobanca.org.ec/wp-content/uploads/2022/08/ESTRATEGIA-NACIONAL-DE-CIBERSEGURIDAD-DEL-ECUADOR-2022481.pdf

OMPI. (s.f.). *Convenio de París para la Protección de la Propiedad Industrial*. Obtenido de Organización Mundial de la Propiedad Intelectual: https://www.wipo.int/treaties/es/ip/paris/

OMPI. (s.f.). *Convenio para la protección de los productores de fonogramas contra la reproducción no autorizada de sus fonogramas*. Obtenido de Organización Mundial de la Propiedad Intelectual: https://www.wipo.int/treaties/es/ip/phonograms/

OMPI. (s.f.). *Reseña del Convenio de Berna para la Protección de las Obras Literarias y Artísticas (1886)*. Obtenido de Organización Mundial de la Propiedad Intelectual: https://www.wipo.int/treaties/es/ip/berne/summary_berne.html

Ortiz Campos, N. (2019). Normativa Legal sobre Delitos Informáticos en Ecuador. *Dialnet, Vol. 4*(Nº. 1), 100-111. doi:file:///C:/Users/Usuario/Downloads/Dialnet-NormativaLegalSobreDelitosInformaticosEnEcuador-7148227.pdf

Quintero, R. D. (s.f). DELITOS INFORMATICOS. *De Sola Pate & Brown.* doi:file:///C:/Users/Usuario/Downloads/DELITOS_INFORMATICOS.pdf

Ramirez, R. (27 de diciembre de 2017). *Delitos informáticos establecidos en el COIP y como prevenirlos.* Obtenido de Policia Nacional del Ecuador: https://www.policia.gob.ec/delitos-informaticos-establecidos-en-el-coip-y-como-prevenirlos/

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

Sandoval, F. (16 de agosto. de 2016). En Ecuador, el 85% de los delitos informáticos ocurre por descuido del usuario. *EL TELEGRAFO*. Obtenido de https://www.eltelegrafo.com.ec/noticias/judicial/1/en-ecuador-el-85-de-los-delitos-informaticos-ocurre-por-descuido-del-usuario

Sosa Meza, J. (24 de noviembre de 2005). *Aspectos generales y comparados de la Ley de Comercio Electrónico*. Obtenido de DerechoEcuador.com: https://derechoecuador.com/aspectos-generales-y-comparados-de-la-ley-de-comercio-electroacutenico/

United Nations. (2021). *COVID-19 AND E-COMMERCE A GLOBAL REVIEW.* New York: United Nations Publications. Obtenido de https://unctad.org/system/files/official-document/dtlstict2020d13_en_0.pdf

Zambrano, J., Dueñas Zambrano, K., & Macías Ordoñez, L. (s.f.). Delito Informático. Procedimiento Penal en Ecuador. *Dominio de las ciencias*, 204-215. Obtenido de file:///C:/Users/Usuario/Downloads/Dialnet-DelitoInformaticoProcedimientoPenalEnEcuador-5761561.pdf