UNIVERSIDAD REGIONAL AUTÓNOMA DE LOS ANDES

"UNIANDES"

FACULTAD DE JURISPRUDENCIA

CARRERA DE DERECHO

ARTÍCULO CIENTÍFICO PREVIO A LA OBTENCIÓN DEL TÍTULO DE ABOGADA

TEMA: EL DELITO DE ESTAFA EN REDES SOCIALES Y EL IMPACTO EN LA SOCIEDAD ECUATORIANA

AUTORA: ARMIJOS ZHINDON YEALINNE CAROLINA

TUTOR: DR. NEVÁREZ MONCAYO JUAN CARLOS.

Santo Domingo – Ecuador

2023

APROBACIÓN DEL TUTOR DEL TRABAJO DE TITULACIÓN

CERTIFICACIÓN:

Quien suscribe, legalmente **CERTIFICA QUE**: El presente Trabajo de Titulación realizado por la **Srta. ARMIJOS ZHINDON YEALINNE CAROLINA,** estudiante de la carrera de Derecho, Facultad de Jurisprudencia, con el tema "**EL DELITO DE ESTAFA EN REDES SOCIALES Y EL IMPACTO EN LA SOCIEDAD ECUATORIANA"**, ha sido prolijamente revisado, y cumple con todos los requisitos establecidos en la normativa pertinente de la Universidad Regional Autónoma de Los Andes -UNIANDES- por lo que apruebo su presentación.

Santo Domingo, enero del 2023

Firmado electrónicamente por:

JUAN CARLOS NEVAREZ MONCAYO

DR. NEVÁREZ MONCAYO JUAN CARLOS, MSc.

TUTOR

UNIVERSIDAD REGIONAL AUTÓNOMA DE LOS ANDES
UNIANDES
BIBLIOTECA

DECLARACIÓN DE AUTENTICIDAD

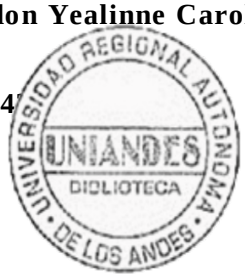
Yo, **ARMIJOS ZHINDON YEALINNE CAROLINA,** estudiante de la carrera de Derecho, Facultad de Jurisprudencia, declaro que todos los resultados obtenidos en el presente trabajo de investigación, previo a la obtención del título de **ABOGADA,** son absolutamente originales, auténticos y personales; a excepción de las citas por lo que son de mi exclusiva responsabilidad.

Santo Domingo, enero del 2023

Armijos Zhindon Yealinne Carolina

C.C. 230024614

AUTORA



DERECHOS DE LA AUTORA

Yo, **ARMIJOS ZHINDON YEALINNE CAROLINA,** declaro que conozco y acepto la disposición constante en el literal d) del Art. 97 del Estatuto de la Universidad Regional Autónoma de los Andes, que en su parte pertinente textualmente dice: El patrimonio de la UNIANDES, está constituido por: La propiedad intelectual sobre las investigaciones, trabajo científicos o técnicos, proyectos profesionales y consultaría que se realicen en la Universidad o por cuenta de ella.

Santo Domingo, enero del 2023

Armijos Zhindon Yealinne Carolina

C.C. 2300246143

AUTORA

TEMA

"EL DELITO DE ESTAFA EN REDES SOCIALES Y EL IMPACTO EN LA SOCIEDAD ECUATORIANA"

RESUMEN

El Código Orgánico Integral Penal contempla un instituto jurídico del tipo penal, que se relaciona con la estafa a través de redes sociales, sancionando a la persona que utilice sistemas informáticos o redes electrónicas y redes de comunicación fraudulentas que faciliten apropiarse de bienes ajenos o que instigue la transferencia de bienes, valores o derechos sin el consentimiento de la persona próxima o de un tercero, en beneficio propio o los demás. En este sentido, la presente investigación tuvo como objetivo determinar las diferentes modalidades de estafa por medio de las redes sociales y el impacto que esto ha causado en los habitantes del cantón Santo Domingo. La metodología utilizada fue la cuali-cuantitativa; ya que, por medio de las entrevistas a varios profesionales del derecho especialistas en la materia, más los datos estadísticos, se logró obtener los resultados esperados, los mismos que avalaron la propuesta de la investigación. Las conclusiones del presente estudio nos condujeron a determinar la necesidad de incorporar la estafa a través de redes sociales en el Código Orgánico Integral Penal, dado que, no existe el delito de estafa en redes sociales tipificado de manera expresa en la normativa penal ecuatoriana, dejando en la impunidad la sanción de este delito.

Palabras clave: Estafa, redes sociales, delitos informáticos, medios electrónicos.

THEME

"THE CRIME OF SCAM IN SOCIAL NETWORKS AND THE IMPACT IN ECUADORIAN SOCIETY"

RESUME

The Organic Comprehensive Criminal Code contemplates a legal institute criminal type, which is related to the fraud through social networks, penalizing the person who uses computer systems or electronic networks and fraudulent communication networks that facilitate the appropriation of other people's goods or that instigates the transfer of these ones, values or rights without the consent of the person close or of a third party, for their own benefit or others. In this sense, the present research had as objective to determine the different modalities of fraud through social networks and the impact that this has caused in the inhabitants of the canton Santo Domingo. The methodology used was qualitative-quantitative; Because through interviews to various legal professional specialists in the field, and statistical data, it was possible to obtain the expected results, same ones that approved the research proposal. The conclusions of this current study led us to determine the need to incorporate fraud through social networks in the Organic Criminal Comprehensive Code, given that there is no crime of fraud in social networks expressly typified in Ecuadorian criminal law, leaving in impunity the sanction of this crime.

Keywords: Fraud, social networks, computer crimes, electronic media.

INTRODUCCIÓN

Según el diccionario del autor (Cabanellas, 1993), la estafa es el delito de obtención de lucro mediante engaño, ignorancia o abuso de confianza de una persona hacia otra.

El Código Orgánico Integral Penal en el artículo 186, define como estafa a: la persona que, con el fin de obtener un beneficio económico para sí o para un tercero, engañe presentando hechos falsos o falsificando u ocultando hechos reales, con el fin de cometer un hecho que dañe su propiedad o dañe a un tercero. de daños a terceros. (Código Orgánico Integral Penal, 2020)

De manera general, se puede conceptualizar al delito como un hecho antijurídico cometido por una persona, imputada, y castigada con una pena; entonces, la estafa a través del uso de plataformas electrónicas se circunscribe en una figura de tales características, de las tipificadas en el COIP, pero sin mayor esfuerzo de claridad, en tanto, su acepción no es específica al determinar la estafa en redes sociales como un delito ni siquiera informático.

Es menester conocer los antecedentes del delito de estafa partiendo desde los delitos informáticos, pues en la actualidad la sociedad tiene toda información de su vida cotidiana en las plataformas digitales, plataformas que día a día se vuelven más importante para el desarrollo de los países. Para (Ayala & Gonzalez, 2015) las transacciones comerciales, las comunicaciones, los procesos industriales, la investigación, la seguridad, la salud, la justicia, etc., son aspectos que dependen cada día más del adecuado desarrollo de la tecnología informática.

En 1983, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) comenzó a estudiar la posibilidad de aplicar y armonizar el derecho penal a nivel internacional para combatir el uso de las redes informáticas para la delincuencia. Las posibles consecuencias económicas del ciberdelito, su carácter internacional y en ocasiones transnacional y el peligro de que la defensa penal en diferentes países pueda obstaculizar el flujo de información internacional han dado lugar a un intercambio de puntos de vista y propuestas de solución. Sobre la base de actitudes y consideraciones, se realiza una evaluación legal analítica y comparativa de las leyes nacionales aplicables y las propuestas de reforma. Las conclusiones jurídicas políticas conducen en general, la lista de medidas que los países pueden considerar.

Así, en 1986, la OCDE publicó el informe "Delito informático: un análisis de leyes y reglamentos", en el que se esbozaban las disposiciones legales existentes y se proponían reformas en cada estado miembro, además de sugerir una lista de ejemplos de uso inapropiado. lista mínima. Se pueden prohibir y sancionar sanciones (lista mínima), tales como fraude y uso indebido de programas informáticos, manipulación informática, alteración de datos y programas informáticos, sabotaje informático, acceso no autorizado, interceptación no autorizada y copia no autorizada de programas informáticos protegidos. (Pino, 2016)

Dado el avance de las tecnologías de la información y su impacto en casi todos los ámbitos de la vida social, han surgido algunas conductas ilícitas, comúnmente conocidas como delitos electrónicos o delitos informáticos, aunque existe un tipo de delito en el derecho penal ecuatoriano, pero no se cumple. porque la conducta detectada no cuenta con los medios para actuar sobre ella, es decir, por medios electrónicos.

El phishing se configura como una de las conductas fraudulentas con más repercusión en la actualidad. Se trata de una práctica encuadrada en el campo de la estafa, que consiste en la adquisición de información confidencial (de carácter económico, personal, o de cualquier otra índole) de forma ilícita, sin consentimiento de su titular; mediante el uso de ingeniería social.

El infractor, conocido como phisher, puede simular ser una persona o empresa de confianza, cometiendo el hecho ilícito mediante una comunicación electrónica aparentemente normal (correo electrónico, mensajería instantánea) o incluso, mediante una llamada telefónica. La persona que lleva a cabo esta actividad delictiva suele camuflarse bajo el nombre de la entidad bancaria habitual u otros servicios contratados por el sujeto engañado con el fin de conseguir códigos, contraseñas, números de tarjetas de crédito u otro tipo de información, especialmente bancaria. (Sánchez, 2009)

Es importante describir que es el delito informático, por lo que, para (Ojeda, 2016), en su libro sobre derecho informático, se define como "actitud contraria a los intereses de las personas que utilizan la computadora como herramienta o fin (término atípico), o una actividad típica, ilegal o delictiva (término típico) de usar la computadora como un medio o fin (término típico).

Referente a los delitos en redes sociales (Artigas & Casanova, 2020) refieren que con el desarrollo de oportunidades de interacción global utilizando las tecnologías de la información y la comunicación, especialmente las redes sociales, se genera vulnerabilidad de estos sistemas de gestión de la información, la preparación insuficiente y la falta de medidas preventivas y educativas, las personas y organizaciones están expuestas a un mayor desarrollo y peligros del ciberdelito, por lo que es importante comprender el contexto anterior, las consecuencias de los delitos informáticos y la normativa vigente en el país para encontrar posibles respuestas o enfoques prevención y tratamiento.

Las redes sociales se están convirtiendo en un fenómeno creciente utilizado por cada vez más personas, pero a su vez son utilizadas por los ciberdelincuentes para obtener artículos o portar herramientas para llevar a cabo sus actividades delictivas. Todo esto se debe al enorme potencial que tienen estas redes debido al gran flujo de información, bienes y datos, ya que los delincuentes explotan el exceso de confianza y los errores de los usuarios para lograr sus objetivos.

La Constitución de la República del Ecuador es la Norma Suprema del Estado, y en esta se contempla que, el derecho a administrar justicia es un derecho del pueblo y es ejercido por la función judicial y otros órganos y funciones según lo prescrito en la Constitución. De tal forma que, el delito de estafa en redes sociales y el impacto en la sociedad ecuatoriana, es una institución penal cuya acción se inicia con el rol que ejerce la fiscalía general del Estado en esta materia. (Constitución de la República del Ecuador, 2008).

En ese sentido, la Fiscalía, de acuerdo con la Constitución, dirigirá, de oficio o a petición de una de las partes, investigaciones y procesos penales. Durante el juicio, ejercerá la acción pública siguiendo los principios de publicidad y mínima injerencia delictiva, con especial atención al interés público y los derechos de las víctimas. De ser meritorio, acusará a los presuntos autores ante un juez competente, y sustentará la acusación en el curso del proceso penal.

Dentro del COIP existe una figura del tipo penal, que se relaciona con la estafa a través de redes sociales, esta señala que, la persona que utilice sistemas informáticos o redes electrónicas y redes de comunicación fraudulentas que faciliten apropiarse de bienes ajenos o que instigue la transferencia de bienes, valores o derechos sin el consentimiento

de la persona próxima o de un tercero, en beneficio propio o los demás, serán sancionados con prisión de uno a tres años. (Código Orgánico Integral Penal, 2020).

Mediante un boletín de prensa la Fiscalía General del Estado el 19 de febrero de 2020, en primera instancia condenan a Elikan M. con trece años de prisión y el pago de una indemnización de $926 990, el cual a través de publicidad en buses, folletos y en una página electrónica, ofrecía planes de inversión con ganancias de hasta treinta veces más, en planes de corto, mediano y largo plazo.

Sin embargo, el pago de capital y rendimientos no se cumplieron desde el 2015, aproximadamente. El 9 de febrero de 2017, los inversionistas recibieron en sus correos electrónicos personales una notificación que les informaba el cierre de la empresa Efexco Cía. Ltda. y de esta manera daban por concluidas sus operaciones en Quito, sin indicar las fechas o formas de devolución del dinero captado. (Fiscalía General del Estado, 2020)

En la actualidad es muy común el delito de estafa a través de redes sociales, ya que es más fácil llegar a la sociedad por estos medios, al encontrarnos en un mundo digitalizado.

Según denuncias presentadas en las Fiscalías de Ecuador, el país registró 8.421 casos de ciberdelincuencia en el año 2017; estos números aumentaron en el año 2018 a 9,571 denuncias y 10,279 respectivamente en 2019. Hay que considerar que hay una tendencia de crecimiento continuo referente a los delitos cibernéticos. (El Universo, 2020)

Elementos conceptuales

Red social

Según (Aguirre, 2011), una red social es un conjunto de lazos que existen entre varios individuos cuya función principal es explicar uno o más comportamientos sociales entre los miembros que forman los lazos.

Estafa

En general, el fraude puede ser descrito como el hecho de que una persona se apropia indebidamente de un bien debido al hecho ilícito de un agente que pretende transformar dicho acto en beneficio propio o de un tercero. La causa de la estafa, como la de sus derivados, es esta: El agente incurre en actividad fraudulenta que induzca a error a una

persona que, como consecuencia de ese error, preste servicios en perjuicio de la propiedad. Por tanto, la conducta punible es el fraude por medios engañosos. (Creus, 1999)

Delitos a través de redes sociales

Según (Morocho, 2022), actualmente no existe una regulación para los delitos de estafa cometidos a través de las redes sociales. Aunque comparten características clave, hay dos razones principales por las que las reglas no prevén sanciones. Una es que se desconoce el paradero del sujeto al cometer dichos delitos; estas personas son muy cuidadosas para cobrar, suelen hacerlo en nombre de un tercero, asegurándose de que son independientes de cualquier actividad ilegal de la que se les pueda acusar.

Estado actual del problema

La importancia y actualidad del tema investigado, se refleja precisamente en los altos índices de delitos en redes sociales que se han presentado en la ciudad de Santo Domingo, durante el año 2021, de cuya información preliminar se tiene que, en la mayoría de los casos, las víctimas no han presentado la respectiva denuncia en la fiscalía, y en otros, que se conoce que sí lo han hecho, se han dilatado las investigaciones, sin tener mayor respuesta por parte del organismo del Estado.

Objetivo General

La presente investigación tuvo como objetivo determinar los niveles de incremento y las diferentes modalidades de delitos de estafa a través de redes sociales y el impacto causado en la sociedad ecuatoriana.

Lineamientos de la Investigación

En cuanto a los parámetros que se observaron durante este trabajo de investigación en la Universidad Regional Autónoma de los Andes, según el libro: “La Investigación Científica y las Formas de Titulación Aspectos Conceptuales y Prácticos”, se puede apreciar que este trabajo científico adopta las siguientes direcciones de investigación:

- Retos, Perspectivas y Perfeccionamiento de las Ciencias Jurídicas en Ecuador.

- ✓ Fundamentos técnicos y doctrinales de las ciencias penales en Ecuador. Tendencias y perspectivas.

Campo de investigación y objeto de estudio

La investigación se desarrolló en el derecho penal y el objeto de estudio es la estafa a través de redes sociales y el impacto que causa en la sociedad ecuatoriana.

MATERIALES Y MÉTODOS

El enfoque o método de investigación desarrollado fue cuali-cuantitativo, y diseñado para el tipo de información que se va a recopilar, se consideró todos los aspectos sobre el delito de estafa a través de redes sociales. Se pudo recolectar información de varias fuentes bibliográficas que se relacionan con el problema tratado en la investigación, así mismo se verificó en la legislación nacional, derecho comparado, doctrina, jurisprudencia, trabajos investigativos referente a la temática desarrollada.

Alcances de la investigación

Exploratoria: La investigación exploratoria tiene características que ayudaron a este trabajo de investigación, a saber, identificar conceptos y priorizar puntos de vista clave, se enfoca en el conocimiento completo del tema, por lo que las opiniones, es decir, puntos de vista únicos y no considerados, pueden haberse obtenido antes del estudio explicativo de la relación. busca la causalidad de dicho tópico. En este sentido, a nivel de descubrimiento, como lo ha señalado Gomez, et al (2017), se analizan tópicos poco abordados en el pasado.

Descriptiva: A través de la investigación descriptiva se analizó cómo es y cómo se manifiesta el delito de estafa a través de redes sociales en el Ecuador, y qué impacto causa en la sociedad ecuatoriana.

Métodos

Método Exegético: La aplicación de la exégesis del conocimiento se vuelve imperiosa en la presente investigación, en tanto, será necesario desentrañar el espíritu del legislador, acerca del conocimiento de la norma utilizando diversas técnicas, lo que implica que se pueda llegar a conclusiones disímiles sobre el delito de estafa a través de redes sociales.

Método deductivo: Se aplicará el método deductivo, ya que en el artículo científico se investiga, partiendo desde la problemática general, a decir de los efectos que causan los delitos a través de redes sociales, frente a la actuación estatal para combatirlo.

Método analítico – sintético: Se utilizará el método analítico-sintético, ya que, al utilizar fuentes de información teóricas como juicios, resoluciones o sentencias, normativas, entrevistas, etc., se requiere un proceso investigativo para descomponer toda esta información en ideas principales y contenidos específicos, en lo relacionado a la estafa a través de redes sociales.

Análisis documental: Este análisis está relacionado al procesamiento y recopilación de información contenida en determinados documentos (archivos y gacetas judiciales) y que no son parte constitutiva de las fuentes bibliográficas expresadas en artículos, ensayos y libros, también necesarios en una investigación.

Técnicas

Entrevistas: "Es una técnica de recolección de datos sobre un determinado tema de opinión, mediante el uso de modelos aplicados a una muestra unitaria de la población" (Muñoz, 2011). El diseño del cuestionario se basó en preguntas específicas para obtener las opiniones de los entrevistados y así obtener respuestas confiables.

Las entrevistas se aplicaron a los Jueces de la Unidad Judicial Penal; Abogados especialistas en materia penal; Abogados de la Defensoría Pública y fiscales.

RESULTADOS

Normativa ecuatoriana

LEGISLACIÓN ECUATORIANA	
Normas constitucionales	**Art. 46 numeral 7. -** El Estado adoptará, entre otras, las siguientes medidas que aseguren a las niñas, niños y adolescentes: 7. Protección frente a la influencia de programas o mensajes, difundidos a través de cualquier medio, que promuevan la

	violencia, o la discriminación racial o de género. Las políticas públicas de comunicación priorizarán su educación y el respeto a sus derechos de imagen, integridad y los demás específicos de su edad. Se establecerán limitaciones y sanciones para hacer efectivos estos derechos.
	Art. 66 numerales 6, 7 y 19 - Se reconoce y garantizará a las personas: 6. El derecho a opinar y expresar su pensamiento libremente y en todas sus formas y manifestaciones. 7. El derecho de toda persona agraviada por informaciones sin pruebas o inexactas, emitidas por medios de comunicación social, a la correspondiente rectificación, réplica o respuesta, en forma inmediata, obligatoria y gratuita, en el mismo espacio u horario. 19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.

	Art. 75.- Toda persona tiene derecho al acceso gratuito a la justicia y a la tutela efectiva, imparcial y expedita de sus derechos e intereses, con sujeción a los principios de inmediación y celeridad; en ningún caso quedará en indefensión. El incumplimiento de las resoluciones judiciales será sancionado por la ley

Normas Legales	**Código Orgánico Integral Penal** **<u>Art. 186.- Estafa.-</u>** La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años. **<u>Artículo 190.-</u>** Apropiación fraudulenta por medios electrónicos.- La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años. La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de

	tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes. **Artículo 191.-** Reprogramación o modificación de información de equipos terminales móviles.- La persona que reprograme o modifique la información de identificación de los equipos terminales móviles, será sancionada con pena privativa de libertad de uno a tres años. **Artículo 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, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años. **Artículo 230.-** Interceptación ilegal de datos.- Será sancionada con pena privativa de libertad de tres a cinco años: 1. La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato

	informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible. 2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder. 3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares. 4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.

Fuente: (Constitución de la República del Ecuador, 2008) (Código Orgánico Integral Penal , 2021)

Autora: Elaboración propia.

En la actualidad existen diferentes cyber delitos como:

Hackeo: Se trata de obtener acceso no autorizado a un sistema informático infringiendo sus mecanismos de seguridad específicos, es decir, que no modifica ni manipula los datos a los que ha tenido acceso.

Cracking: para los autores (Mata & R., 2001), sabotaje informático" incluye la manipulación de programas para hacer que se bloqueen o colapsen, la actividad ilegal ocurre al destruir el bien intangible que es la información, borrándola o moviéndola con el fin de hacer colapsar la plataforma en la que se encuentran.

Grooming: Implica en persuadir al usuario para que comparta imágenes pornográficas de sí mismo, y luego el destinatario chantajea a la víctima exigiendo más imágenes o dinero para evitar que las publique en línea.

Resultados en Derecho Comparado

Legislación de Colombia: Los delitos informáticos son actividades ilegales cometidas a través del espacio digital, el entorno digital o Internet. En Colombia, el delito informático se puede definir como el acceso ilegal o no autorizado a datos e información protegidos en forma digital. (World Legal Corp, 2021)

Estos actos están descritos en la Ley 1273 de 2009 en el artículo 269 literal i y j manifiesta:

i) Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos. (LEY 1273 DE 2009 , 2009)

j) Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave. (LEY 1273 DE 2009 , 2009)

Legislación Argentina: La Ley 26.388 introduce en el código penal argentino una serie de delitos considerados "delitos informáticos". Además, se ha modificado varias

categorías existentes para incorporar nuevos términos de comisión electrónica. Por lo tanto, se agregó el párrafo 16 al artículo 173, que establece: "El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o a la trasmisión de datos". (Ley 26.388, 2008)

Resultados de Doctrina

Los autores (Mora, Sánchez, González, & Quintero, 2017), la legislación sobre delitos cibernéticos protege los bienes legítimos, como los intereses relevantes de las personas como sujetos de la sociedad, que se consideran particularmente valiosos y, por lo tanto, merecedores de protección penal contra acciones que los perjudiquen o amenacen.

Un elemento esencial de la ley penal es la determinación de la pena para la persona o personas responsables de tal delito, si se prueba la existencia de ciertos elementos como: La tipicidad, antijuricidad y culpabilidad, se determinará la conducta punible, independientemente de su naturaleza, y si se debe imponer un castigo, por lo que se debe tipificarla.

En la actualidad, se debe ampliar la tipificación de los delitos informáticos, ya que de esta manera habría una sanción clara y precisa para aquellos que tienen como objetivo afectar los bienes, el honor e incluso la vida de las personas. La tipificación de los delitos informáticos en el derecho penal corresponde a los siguientes elementos: Sujeto: Autor de la conducta ilícita o delictiva; Medio: El sistema informático y Objeto: El bien que produce el beneficio económico o ilícito. (Mora, Sánchez, González, & Quintero, 2017)

El autor (Lux, 2017) manifiesta a detalle que uno de los elementos de suma importancia para considerarse en el momento de establecer la normativa es el bien jurídico, ya que este cumple funciones relevantes.

Por un lado, existen argumentos para suponer que el delito informático protege bienes jurídicos específicos, propiamente informáticos y distintos a los protegidos por las leyes penales tradicionales. Entonces, de acuerdo con este enfoque, la diferencia entre los delitos informáticos y otros delitos es de fondo, no solo de forma. Una consecuencia de esta teoría es a menudo la propuesta de normas de derecho penal, incluso al margen de otras normas diseñadas para proteger de forma independiente estos intereses particulares. (Lux, 2017)

Resultado de las entrevistas

Preguntas	Respuestas
¿Cuál es la respuesta de las autoridades estatales frente a los delitos de estafa a través de redes sociales, y cuál es el alcance de la ley para sancionar los mismos?	Los organismos estatales brindan los canales necesarios para realizar las denuncias por estafa, sin embargo, la estafa a través de redes sociales no ha sido considerada como tal, y lo estipulado en el COIP, no es tan amplio ni claro para sancionar a los delitos informáticos como tal.
¿Cuáles considera usted que serían las diferentes modalidades de delitos de estafa que en la actualidad se están dando a través de redes sociales?	Con los avances tecnológicos existen muchas modalidades, ahora se crean programas con links los cuales una vez que los abres se apropian de tus datos personales, claves, etc., y de está manera se apropian de tu dinero.
¿Cree usted que, existe algún tipo de protección respecto a la estafa por redes sociales del ente estatal con la ciudadanía?	Se considera que el estado en este tema no ha realizado la normativa necesaria y específica para sancionar a las personas que han sido estafadas por redes sociales con las diferentes modalidades, por ende, si sería necesario incorporar al COIP articulado específico sobre este tema.
¿Considera usted que existen falencias o vacíos en la norma que tipifica el delito de estafa través de redes sociales en el COIP?	Como se ha dicho en líneas anteriores, se considera que en efecto existen vacíos legales respecto a esta nueva conducta punible.
¿Cree usted que la legislación de otros países, respecto del delito de estafa a través de redes sociales, aporten significativamente a generar cambios en nuestro ordenamiento jurídico?	Si, ya que legislaciones como Colombia y Argentina en sus Códigos Penales tienen articulados específicos para sancionar este delito, por lo que sería importante que nuestro país las acoja.
¿Está usted de acuerdo en que, en el Código Orgánico Integral Penal se establezca la estafa informática a través de redes sociales, como un delito	Totalmente de acuerdo.

independiente al tipo de estafa contemplada en este?

Fuente: Entrevista aplicada
Elaborado por: Elaboración propia

DISCUSIÓN

(Mata & R., 2001) manifiesta que es necesario presentar ciertas pruebas para poder hablar de ciber estafa, entre ellas están: El afán de lucro, que se manifiesta en la apropiación del patrimonio. Un acto típico de manipulación de un sistema informático es decir que la intención es cambiar el curso normal de un programa implementado para producir un resultado diferente al que se pretendía en el momento de la implementación. La transferencia de propiedad personal sin consentimiento y sin uso de violencia. Y, por último, los daños a terceros por la necesidad de probar que el autor es quien utilizó el criterio de la víctima para cometer el delito.

Tanto la norma suprema como la Constitución de la República como el Código Orgánico Integral Penal protegen el bien jurídico, sin embargo, respecto a los delitos de estafa por redes sociales no hay una norma específica que este tipificada y que sancione este hecho antijurídico, por lo que se desprende que existen vacíos legales sobre esta problemática, a pesar de que en la actualidad se está suscitando la estafa por redes sociales no se ha propuesto una reforma al COIP.

En el derecho comparado se puede ver que, si existen los delitos informáticos como tal, y se describe a los realizados por medio de redes sociales, por lo que, las personas afectadas pueden denunciar este acto punible sin necesidad de adecuarlo a otro como en el COIP, que habla del delito de estafa de manera general.

Las entrevistas realizadas ayudaron a que se abalice el objetivo y problemática planteada, ya que en efecto reconocen que en la actualidad se esta dando con mayor frecuencia la estafa por redes sociales, sin embargo, muchas personas no denuncian ya que no saben a que delito tipificarlo como tal, por lo que se ve necesario incorporar articulado al COIP respecto a este tema.

También es importante destacar que tanto las instituciones como la ciudadanía no tienen bien definido un método de investigación para este tipo de delitos, y que existen muy

pocos profesionales especializados en esta área, y al momento de querer ir a denunciar a fiscalía no proporcionan una mayor información por lo que las personas prefieren ya no hacerlo.

CONCLUSIONES

La ciberdelincuencia está en constante evolución y el nuevo contexto en el que interactúan exige la tipificación de los delitos cometidos utilizando la tecnología. El Código Orgánico Integral Penal, ha logrado grandes avances respecto a ciertos delitos informáticos, pero es necesario revisarlo con regularidad para mantenerlo al día con el ritmo al que surgen nuevas ciber estafas.

El delito de estafa es uno de los delitos que afectan los bienes de las personas, aunque se ha encontrado que la estafa reúne elementos que constituyen el tipo antijurídico, el uso de las tecnologías informáticas hace que está se vuelva impredecible para evitarla.

Finalmente se evidencia que es necesario incorporar el delito de ciber estafa o estafa por redes sociales, ya que hay ciertos vacíos legales en la normativa penal respecto a esta problemática, para que de esta manera tanto las personas afectadas como las instituciones encargadas de sancionar estos delitos tengan claro, el procedimiento a seguir, para que no quede en la impunidad.

Bibliografía

Aguirre, J. (2011). *Introducción al análisis de redes sociales.* Documentos de Trabajo del Centro Interdisciplinario para el Estudio de Políticas Públicas.

Artigas, W., & Casanova, I. (2020). *Influencia de las redes sociales académicas en la construcción de la identidad digital latinoamericana. En Anales de Documentación.* Murcia: Faculta de comunicación y documentación y Servicio de Publicaciones de la Universidad de Murcia.

Ayala, E., & Gonzalez, S. (2015). *Tecnologías de la Información y la Comunicación.* Lima Perú: Universidad Inca Garcilaso de la Vega.

Cabanellas, G. (1993). *Diccionario Jurídico Elemental .* Buenos Aires: Heliasta.

Código Orgánico Integral Penal . (2021). *Código Orgánico Integral Penal .* Quito : Corporación de Estudio y Publicaciones.

Código Orgánico Integral Penal. (2020). *Código Orgánico Integral Penal.* Quito: Corporación de Estudios y Publicaciones.

Constitución de la República del Ecuador. (20 de Octubre de 2008). Registro Oficial No. 449. Quito, Ecuador: Ediciones Legales. Obtenido de http://lexis.uniandesec.elogim

Creus, C. (1999). *Derecho Penal.* Buenos Aires: Astre.

El Universo. (27 de octubre de 2020). *Redes sociales son el nicho ideal para los ciberdelitos en Ecuador*. Obtenido de https://www.eluniverso.com/noticias/2020/09/27/nota/7991326/delitos/

Fiscalía General del Estado. (19 de febrero de 2020). *Sentencia por estafa masiva, ratificada*. Obtenido de https://www.fiscalia.gob.ec/sentencia-por-estafa-masiva-ratificada/

Gomez, C., Alvarez, G., Romero, A., Castro, F., Vega, V., Comas, R., & Velasquez, M. (2017). *La investigacion Cientifica y las Formas de Titulacion.* Quito, Ecuador: Editorial Juridica del Ecuador.

LEY 1273 DE 2009 . (2009). *LEY 1273 DE 2009 .* Colombia.

Ley 26.388. (2008). *CODIGO PENAL.* Argentina.

Lux, L. M. (2017). El bien jurídico protegido en los delitos informáticos. *Revista chilena de derecho*, 261-285.

Mata, & R., M. (2001). *Delincuencia informática y Derecho penal.* Madrid: Edisofer.

Mora, E., Sánchez, Y., González, O., & Quintero, D. (2017). *Los Delitos Informáticos: Experiencia Investigativa en CENDITEL.* Conocimiento Libre y Licenciamiento.

Morocho, G. (2022). *Incidencia del delito de estafa a través del uso de redes sociales, año 2017-2020.* La Libertad: La Libertad: Universidad Estatal Península de Santa Elen.

Ojeda, J. (2016). Delitos informáticos y entorno jurídico vigente en Colombia. . *Cuadernos de Contabilidad*, 41-66.

Pino, S. A. (2016). *Delitos Informáticos: Generalidades.* Guadalajara México: UDG Virtual.

Sánchez, J. (2009). El bien jurídico protegido en el delito de estafa informática. *El bien jurídico protegido en el delito de estafa informática*, 105-121.

World Legal Corp. (30 de junio de 2021). *Delitos informáticos en Colombia*. Obtenido de https://www.worldlegalcorp.com/blog/delitos-informaticos-en-colombia/